08-30-00

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION TRANSMITTAL LETTER	ATTORNEY DOCKET NO.: 10746/20

Address to:
Commissioner of Patents and Trademarks
Washington D.C. 20231
Box Patent Application

Transmitted herewith for filing is the patent application of

Inventor(s): **Hideki AKASHIKA, Shinichi HIRATA, Nagaaki OHYAMA and Akio KOKUBU**

For : **DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM**

Enclosed are:

1. **37** sheets of specification, **35** sheets of claims, and **1** sheet of abstract.
2. **16** sheet(s) of drawings.
3. Declaration and Power of Attorney.
4. Assignment to **Nippon Telegraph and Telephone Corporation**.
5. An Information Disclosure Statement.

The filing fee has been calculated as shown below:

	NUMBER FILED		NUMBER EXTRA*	RATE ($)	FEE ($)
BASIC FEE					690.00
TOTAL CLAIMS	44	- 20 =	24	18.00	432.00
INDEPENDENT CLAIMS	10	- 3 =	7	78.00	546 00
MULTIPLE DEPENDENT CLAIM PRESENT				260.00	
*Number extra must be zero or larger				TOTAL	1,668.00
If applicant is a small entity under 37 C.F.R. §§ 1 9 and 1.27, then divide total fee by 2, and enter amount here.				SMALL ENTITY TOTAL	

6. Please charge the required application filing fee of **$1,668.00** to the deposit account of **Kenyon & Kenyon**, deposit account number **11-0600**.

7. The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication and during the pendency of this application or credit any overpayment to the deposit account of **Kenyon & Kenyon**, deposit account number **11-0600.**

8. A duplicate of this sheet is enclosed.

Dated: August 29, 2000

By: Edward W Greason

Edward W. Greason, (Reg. No. 18,918)

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Hideki Akashika, a citizen of Japan residing at Koutou-ku, Tokyo-to, Japan, Shinichi Hirata, a citizen of Japan residing at Zushi-shi, Kanagawa-ken, Japan, Nagaaki Ohyama, a citizen of Japan residing at Kawasaki-shi, Kanagawa-ken, Japan and Akio Kokubu, a citizen of Japan residing at Minato-ku, Tokyo-to, Japan have invented certain new and useful improvements in

DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM

of which the following is a specification:-

TITLE OF THE INVENTION

DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a data storing system, an apparatus and a computer readable medium storing a data storing program. More particularly, the present invention relates to a data storing system, an apparatus and a computer readable medium storing a data storing program for storing data such as a program into an IC card and the like by using a telecommunication system and the like.

2. Description of the Related Art

Recently, a data storing system which uses an apparatus having a high level of security such as an IC card is becoming popular. An issuer (an IC card issuer) stores an important data such as a program in the apparatus when the issuer issues the apparatus.

MULTOS is an example of a conventional system wherein a system, called MULTOS-CA, which guarantees data has authority to store a program to a user apparatus (for example, an IC card) for retaining security, and the issuer (IC card issuer) in MULTOS stores the program in the user apparatus. Therefor, there are problems that a data provider (a service provider) which provides a program can not let a user store the program which the data provider provides, and that the data provider can not manage information on storing a program.

In addition, there is no means for knowing that a valid issuer and a valid data provider acknowledges user's operation in which the user adds,

changes, deletes data. Thus, there is a problem that data can not be stored in a user apparatus safely via network and the like.

Therefore, a data provider can store data only in a card which is issued by a specific IC card provider. That is, the data provider can not store data in a card which is issued by an IC card issuer which has no relation to the data provider. Therefore, it is needed that a data provider can store data safely into a card which is issued by any IC card issuer by performing certification with reliability.

SUMMARY OF THE INVENTION

It is an object of the present invention that the card issuer and the service provider equally can store and delete data in a card safely by mutual agreement between the user, the card issuer and the service provider.

Another object of the present invention is that each of the card issuer and the service provider can obtain information on data which is stored in an IC card.

Another object of the present invention is to register and manage the card issuer, the service provider and the user apparatus such that mutual certification can be performed. That is, the object is that the service provider can store data safely to a user apparatus and an issuer which are not any specific apparatus or issuer.

According to a first aspect of the present invention, the above object of the present invention is achieved by a data storing system comprising:

a user apparatus which stores data;

an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

a data providing apparatus which is held by a data provider that provides data;

an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and

a data registration apparatus which is held by a data registrar that registers and manages the data provider;

wherein the user apparatus comprises:

a registration information generation part which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

a registration verification part which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises a registration generation part which generates the registration certificate and sends the registration certificate to the user apparatus.

In the data storing system, the user apparatus may further comprises:

a part which sends the registration certificate and storing data information to the issuing apparatus;

a part which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

a part which verifies that the storing data information corresponds to storing data which is acquired; and

a part which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

the issuing apparatus further comprising:

a part which verifies the registration certificate and the storing data information which are received from the user apparatus;

a part which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

a part which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

a part which verifies a storing authorization which is received from the data providing apparatus; and

a part which sends the storing authorization to the user apparatus when the storing authorization is verified;

the data providing apparatus further comprising:

a part which verifies the storing authorization request;

a part which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

According to a second aspect of the present invention, the above object of the present invention is achieved by an issuing apparatus in a

data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising:

a part which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

a registration generation part which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

According to a third aspect of the present invention, the above object of the present invention is achieved by a data providing apparatus in data storing system which comprises: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises:

a registration information generation part which generates registration information on a key including a user public key or a part of a secret

key, sends the registration information to the issuing apparatus with user information; and

a registration verification part which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises a registration generation part which generates the registration certificate and sends the registration certificate to the user apparatus,

the data providing apparatus comprising:

a part which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

a part which verifies the storing authorization request;

a part which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fourth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium storing program code for causing a data storing system to store data, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus

which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider; the computer readable medium comprising:

registration information generation program code means, provided for the user apparatus, which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

registration verification program code means, provided for the user apparatus, which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

registration generation program code means, provided for the issuing apparatus, which generates the registration certificate and sends the registration certificate to the user apparatus.

The computer readable medium may further comprises:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the issuing apparatus;

program code means, provided for the user apparatus, which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

program code means, provided for the user apparatus, which verifies that the storing data information corresponds to storing data which is

acquired; and

program code means, provided for the user apparatus, which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

program code means, provided for the issuing apparatus, which verifies the registration certificate and the storing data information which are received from the user apparatus;

program code means, provided for the issuing apparatus, which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

program code means, provided for the issuing apparatus, which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

program code means, provided for the issuing apparatus, which verifies a storing authorization which is received from the data providing apparatus; and

program code means, provided for the issuing apparatus, which sends the storing authorization to the user apparatus when the storing authorization is verified;

program code means, provided for the data providing apparatus, which verifies the storing authorization request;

program code means, provided for the data providing apparatus, which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a

storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fifth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising:

program code means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation program code means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

According to a sixth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium storing program code for causing a data providing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data

provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises:

registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus,

the computer readable medium comprising:

program code means which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

program code means which verifies the storing authorization request;

program code means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

As mentioned above, in the present

invention, the user apparatus generates the registration information, sends it to the issuing apparatus with user information. The issuing apparatus stores the received registration information and the user information, provides certificate information to the registration information, generates registration certificate, sends it to the user apparatus. The user apparatus verifies the received registration certificate, stores it in a storage device if it is verified, such that data in an IC card can be stored and deleted safely.

According to the above-mentioned invention, by using the registration certificate which is issued by the registration issuer, the party which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

In addition, the issuing apparatus, the data providing apparatus and the user apparatus verifies the registration certificate, the storing authorization request and the storing authorization such that tampering by a third party is prevented.

Further, each of the card issuer and the service provider can obtain information on data which is stored an IC card.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the present invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings, in which:

Fig.1 is a figure showing the principle of the present invention;

Fig.2 is a block diagram of a data storing

system of the present invention;

Fig.3 is a diagram for explaining a general outline of the operation of the data storing system;

Fig.4 shows a system configuration for user registration according to a first embodiment of the present invention;

Fig.5 is a diagram for explaining a general outline of the operation of the data storing system when data is stored via an issuer according to a second embodiment;

Fig.6 is a block diagram of the data storing system when data is stored via the issuer according to the second embodiment;

Fig.7 is a diagram for explaining a general outline of the operation of the data storing system when data is stored via an data provider according to a third embodiment;

Fig.8 is a block diagram of the data storing system when data is stored via the data provider according to the third embodiment;

Fig.9 is a diagram for explaining a general outline of the operation of the data storing system when data is stored only by the data provider according to a fourth embodiment;

Fig.10 is a block diagram of the data storing system when data is stored only by the data provider according to the fourth embodiment;

Fig.11 is a diagram for explaining a general outline of the operation of the data storing system when a user apparatus is registered according to a fifth embodiment;

Fig.12 is a block diagram of the data storing system when a user apparatus is registered according to the fifth embodiment;

Fig.13 is a diagram for explaining a general outline of the operation of the data storing

system when data is stored according to a sixth embodiment;

Fig.14 is a block diagram of the data storing system when data is stored according to the sixth embodiment;

Fig.15 is a block diagram of the data storing system when data is stored according to a seventh embodiment;

Fig.16 is a block diagram of a computer system which can be used as an issuing apparatus, a data providing apparatus and the like.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig.1 and Fig.2 are figures of a data storing system for explaining the principle of the present invention. The data storing system includes a user apparatus 300 which stores data; an issuing apparatus 100 which is held by an issuer that provides the user apparatus 300, issues and manages a registration certificate; a data providing apparatus 200 which is held by a data provider that provides data; an issuer registration apparatus 400 which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus 500 which is held by a data registrar that registers and manages the data provider.

In the above-mentioned configuration, the user apparatus includes a registration information generation part 320 which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus 100 with user information; and a registration verification part 330 which verifies a registration certificate which is received from the issuing apparatus and which is signature information or a hash value of the issuer for the registration information and the user

information, stores the registration certificate to a storage device 310 when the registration certificate is verified.

The issuing apparatus 100 includes a registration generation part 120 which generates the registration certificate and sends the registration certificate to the user apparatus.

Since the issuer issues the registration certificate to the user apparatus 300, validity of the user apparatus is insured.

As mentioned above, as shown in Fig.2, the data storing system of the present invention includes an issuing apparatus 100, a data providing apparatus 200, a user apparatus 300, an issuer registration apparatus 400 and a data registration apparatus 500. The issuing apparatus 100 is owned by an issuer which provides the user apparatus, issues and manages a registration certificate. The data providing apparatus 200 is owned by a data provider which provides data. The user apparatus 300 stores the registration certificate and the data. The issuer registration apparatus 400 is owned by an issuer registrar which insures validity of the registration certificate. The data registration apparatus 500 is owned by a data registrar which insures validity of data.

Data can be exchanged between these apparatuses, for example, via communication lines, the Internet and the like. A tamperproof apparatus (an IC card and the like) can be used for these apparatuses.

The issuing apparatus 100, the data providing apparatus 200, the issuer registration apparatus 400 and the data registration apparatus 500 generate and retain key information (such as a public key, a private key, a shared key, a part of a secret key and the like) for generating and

verifying a certificate which uses symmetric key cryptography, public key cryptography, digital signature method, secure hash method (message digest) or the like (which can be refereed in "CONTEMPORARY ENCRYPTION THEORY", Ikeno, Koyama, IEICE.

In the following, a general outline of the operation of an embodiment of the present invention will be described with reference to Fig.3. Each of the issuer registration apparatus and the data registration apparatus issues a registration certificate for the issuing apparatus and the data providing apparatus respectively by using a signature or the like. According to the registration certificate, each of the issuing apparatus and the data providing apparatus can be proved to be valid.

The issuing apparatus issues a registration certificate to the user apparatus. An application can be downloaded into the user apparatus via the issuing apparatus or via the data providing apparatus. An authorization for storing data is exchanged between the issuing apparatus and the data providing apparatus.

In the following, embodiments of the present invention will be described with reference to figures.

(first embodiment)

A first embodiment will be described with reference to Fig.4. In this embodiment, the process of user registration between the user apparatus 300 and the issuing apparatus 100 will be described.

Fig.4 shows a system configuration for user registration of the first embodiment. This system includes the issuing apparatus 100 and the user apparatus 300. The issuing apparatus 100 includes a database 110 and a certificate generation

part 120. The certificate generation part 120 generates a digital signature (or encrypted data, or secure hash) for proving that the issuer generates a registration certificate from input data. As the input data, information (RI) on a key such as a user public key (public key, symmetric key in symmetric key cryptography or the like) and user information (UID) which includes a user identifier are input from the user apparatus 300. The certificate generation part 120 generates the digital signature (or encrypted data, or secure hash) of the issuer for the registration information (RI) and the user information (UID) which are input from the user apparatus 300. The registration generation part 120 outputs these data to the user apparatus 300 as a registration certificate (RC). In the above configuration, the issuing apparatus 100 may generate the registration information (RI) and the user information (UI) instead of receiving them from the user apparatus 300. In such a case, the issuing apparatus 100 includes a registration information generation part.

The user apparatus 300 includes a memory 310, a registration information generation part 320 and a certificate verification part 330.

The registration information generation part 320 generates the registration information (RI) and the user information (UID), and stores these information into the memory 310.

The certificate verification part 330 verifies validity of the registration certificate (RC) input from the issuing apparatus 100. The certificate verification part 330 verifies the digital signature (or encrypted data, or secure hash) of the registration certificate (RC). When the registration certificate is valid, the certificate verification part 330 stores the

registration certificate (RC) into the memory 310.

The operation of user registration is as follows.

(Step 11) The registration information generation part 320 in the user apparatus 300 generates the registration information for the issuing apparatus 100, stores the registration information (RI) into the memory 310, and sends the registration information (RI) to the issuing apparatus 100. When the issuing apparatus issues the registration information, this step 11 is not performed.

(Step 12) The certificate generation part 120 in the issuing apparatus 100 generates a registration certificate (RC) from the registration information (RI), stores it in the database 110, and sends it to the user apparatus 300.

(Step 13) The certificate verification part 330 in the user apparatus 300 verifies the registration certificate (RC), and stores the registration certificate (RC) in the memory 310 if it is verified.

(Second embodiment)

In this embodiment, the process of storing data (downloading of application) via the issuer will be described. First, the general outline will be described with reference to Fig.5.

In this process, the data registration apparatus 500 issues a data provider registration certificate to a data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.5.

When the user apparatus 300 requests application download to the issuing apparatus 100 in step 21, the issuing apparatus 100 sends a storing authorization request to the data providing apparatus 200 in step 22. The data providing apparatus 200 issues a storing authorization to the

issuing apparatus 100 in step 23. Then, the issuing apparatus 100 downloads a requested application to the user apparatus 100 in step 24.

Next, the second embodiment will be described in detail with reference to Fig.6. Fig.6 is a block diagram of the data storing system for data storing via the issuer according to the second embodiment.

This system shown in Fig.6 includes a issuing apparatus 100, a data providing apparatus 200 and a user apparatus 300.

The issuing apparatus 100 includes a certificate generation part 120, a certificate verification part 130 and a storing data verification part 140.

The certificate verification part 130 acquires a registration certificate (RC) from the user apparatus 300 and verifies the digital signature (or encrypted data, or secure hash) for proving that the registration certificate (RC) is generated by the issuing apparatus 100. When the registration certificate is verified, a storing authorization is issued, and sent to the user apparatus 300.

The storing data verification part 140 acquires storing data information (SDI) which includes storing data identifier from the user apparatus 300. Then, the storing data verification part 140 verifies the storing data information (SDI). When the data is verified, the verification result (storing data information (SDI)) is sent to the certificate generation part 120 and the data providing apparatus 200.

The certificate generation part 120 receives verified a registration certificate (RC) from the certificate verification part 130 and receives verified storing data information (SDI)

from the storing data verification part 140. Then, the certificate generation part 120 generates a digital signature (or encrypted data, or secure hash) for the registration certificate and the storing data information, and sends the digital signature as a storing authorization request (SAR) to the data providing apparatus 200.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data verification part 240.

When the certificate verification part 230 acquires the storing authorization request (SAR) from the issuing apparatus, the certificate verification part 230 verifies the storing authorization request. When it is verified, the certificate verification part 230 sends the storing data information (SDI) to the storing data verification part 240 and sends the storing authorization request (SAR) to the certificate generation part 220.

The storing data verification part 240 writes the storing data information (SDI) which is received from the certificate verification part 230 into the database 210. In addition, the storing data verification part 240 verifies the storing data information (SDI). When it is verified, the storing data information (SDI) is sent to the certificate generation part 220.

The certificate generation part 220 verifies the storing authorization request (SAR) received from the certificate verification part 230 and verifies the storing data information (SDI) receives from the storing data verification part 240. When they are verified, storing authorization (SA) is sent to the issuing apparatus 100.

The user apparatus 300 includes a memory

310, a certificate verification part 330 and a data verification part 340.

The certificate verification part 330 acquires the storing authorization (SA) from the issuing apparatus 100, verifies it, and sends the verification result to the data verification part 340.

When the storing authorization (SA) is verified in the certificate verification part 330, the data verification part 340 acquires storing data (APD) from the data providing apparatus 210, and writes the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is stored via the issuer will be described in detail.

(Step 21) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the issuing apparatus 100.

(Step 22) The issuing apparatus 100 verifies the registration certificate (RC) in the certificate verification part 130, and verifies the storing data information (SDI) in the storing data verification part 140. When both of them are verified, the issuing apparatus 100 generates the storing authorization request (SAR) in the certificate generation part 120, and sends the registration certificate (RC), the storing data (SDI) and the storing authorization request (SAR) to the data providing apparatus 200.

(Step 23) The data providing apparatus 200 verifies the storing authorization request (SAR) in the certificate verification part 230, and verifies the storing data information (SDI). When both of them are verified, the data providing apparatus 200 generates a storing authorization (SA) for the storing authorization request (SAR) and the storing data information (SDI) in the certificate generation

part 220, and sends the storing authorization (SA) to the issuing apparatus 100.

(Step 24) The issuing apparatus 100 verifies the storing authorization (SA) in the certificate verification part 130. When it is verified, the issuing apparatus sends the storing authorization (SA) to the user apparatus 300.

Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received in some way by using the data verification part 340. When it is verified, the storing data (APD) is stored in the memory 310.

In the above-mentioned process, the user apparatus can delete the storing data (APD) which is already in the memory 310.

(third embodiment)

In the third embodiment, a case wherein data is stored via the data provider. The general outline will be described with reference to Fig.7.

In this embodiment, the data registration apparatus 500 issues a data provider registration certificate to a data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.7.)

When the user apparatus 300 requests application download to the data providing apparatus 200 in step 31, the data providing apparatus 200 sends a storing authorization request to the issuing apparatus 100 in step 32. The issuing apparatus 100 issues a storing authorization to the data providing apparatus 200 in step 33. Then, the data providing apparatus 200 downloads a requested application to the user apparatus 100 in step 34.

Next, the third embodiment will be described in detail with reference to Fig.8. Fig.8

is a block diagram of the data storing system for data storing via the data provider according to the third embodiment.

This system shown in Fig.8 includes a issuing apparatus 100, a data providing apparatus 200 and a user apparatus 300.

The issuing apparatus 100 includes a certificate generation part 120, a certificate verification part 130 and a storing data verification part 140.

When the certificate verification part 130 acquires the storing authorization request (SAR) from the data providing apparatus 200, the certificate verification part 130 verifies the storing authorization request. When it is verified, the certificate verification part 130 sends the storing data information (SDI) to the storing data verification part 140 and sends the storing authorization request (SAR) to the certificate generation part 120.

The storing data verification part 140 verifies the storing data information (SDI). When it is verified, the storing data information (SDI) is sent to the certificate generation part 120.

The certificate generation part 120 sends a digital signature (or encrypted data, or secure hash) as the storing authorization (SA) to the data proving apparatus 200. The digital signature proves that the storing authorization (SA) is generated by the issuer on the basis of the storing authorization request (SAR) received from the certificate verification part 130 and the storing data information (SDI) received from the storing data verification part 140.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data

verification part 240.

The certificate verification part 230 acquires the storing authorization (SA) from the issuing apparatus 100 and acquires a registration certificate (RC) from the user apparatus 300, and verifies them.

The certificate generation part 220 receives the registration certificate (RC) from the certificate verification part 230 and receives the storing data information (SDI) from the storing data verification part 240. Then, the certificate generation part 220 generates a storing authorization request (SAR) from them, and sends the storing authorization request (SAR) to the issuing apparatus 100.

The storing data verification part 240 acquires storing data information (SDI) from the user apparatus 300. Then, the storing data verification part 240 verifies the storing data information (SDI). When it is verified, the verification result (storing data information (SDI)) is sent to the certificate generation part 220.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data verification part 340.

The registration certificate (RC) is sent to the certificate verification part 230 of the data providing apparatus 200 from the memory 310, and the storing data information (SDI) is sent to the storing data verification part 240 of the data providing apparatus 200.

The certificate verification part 330 acquires the storing authorization (SA) from the certificate verification part 230 in the data providing apparatus 230, verifies the storing authorization (SA), and sends the verification result to the data verification part 340 when the

storing authorization (SA) is verified.

The data verification part 340 acquires storing data (APD) from the database 210 in the data providing apparatus 200, and verifies the data. When it is verified, the data verification part 340 stores the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is stored via the provider will be described in detail.

(Step 31) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the data providing apparatus 200.

(Step 32) The data providing apparatus 200 verifies the registration certificate (RC) in the certificate verification part 230, and verifies the storing data information (SDI) in the storing data verification part 240. When both of them are verified, the data providing apparatus 200 generates the storing authorization request (SAR) based on the registration certificate (RC) and the storing data (SDI) in the certificate generation part 220, and sends the registration certificate (RC), the storing data (SDI) and the storing authorization request (SAR) to the issuing apparatus 200.

(Step 33) The issuing apparatus 100 verifies the storing authorization request (SAR) in the certificate verification part 130, and verifies the storing data information (SDI) in the storing data verification part 140. When both of them are verified, the issuing apparatus 100 generates a storing authorization (SA) for the storing authorization request (SAR) and the storing data information (SDI) in the certificate generation part 120, and sends the storing authorization (SA) to the data providing apparatus 100.

(Step 34) The data providing apparatus 200

verifies the storing authorization (SA) in the certificate verification part 230. When it is verified, the data providing apparatus 200 sends the storing authorization (SA) to the user apparatus 300.

Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received in some way by using the data verification part 340. When it is verified, the storing data (APD) is stored in the memory 310.

In the above-mentioned process, the user apparatus 300 can delete the storing data (APD) which is already in the memory 310 instead of storing the storing data (APD).

(fourth embodiment)

In this embodiment, data storing process only by the data provider will be described. The general outline will be described with reference to Fig.9. In this embodiment, authorization by the card issuer may not be necessary for data download.

In this embodiment, the data registration apparatus 500 issues a data provider registration certificate to the data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.9.)

When the user apparatus 300 requests application download to the data providing apparatus 200 in step 41, the data providing apparatus 200 downloads a requested application to the user apparatus 300 in step 42.

Next, the fourth embodiment will be described in detail with reference to Fig.10. Fig.10 is a block diagram of the data storing system for data storing only by the data provider according to the fourth embodiment.

This system shown in Fig.10 includes a

data providing apparatus 200 and a user apparatus 300.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data verification part 240.

The certificate verification part 230 acquires a registration certificate (RC) from the user apparatus 300, and verifies it.

The certificate generation part 220 verifies both of the registration certificate (RC) the storing data information (SDI). When they are verified, the certificate generation part 220 generates a storing authorization request (SAR) from them, and sends the storing authorization request (SAR) to the user apparatus 300.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data verification part 340.

The certificate verification part 330 acquires the storing authorization (SA) received from the data providing apparatus 200, and verifies the storing authorization (SA).

The data verification part 340 acquires storing data (APD) from the data providing apparatus 200, and verifies the data. When it is verified, the data verification part 340 stores the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is stored only by the data provider will be described in detail.

(Step 41) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the data providing apparatus 200.

(Step 42) The data providing apparatus 200

verifies the registration certificate (RC) in the certificate verification part 230. When it is verified, the data providing apparatus 200 generates the storing authorization (RC) based on the storing data information (SDI) in the certificate generation part 220, and sends the storing authorization (RC) to the user apparatus 300.

Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received in some way by using the data verification part 340. When it is verified, the storing data (APD) is stored in the memory 310.

In the above-mentioned process, the user apparatus 300 can delete the storing data (APD) which is already in the memory 310 instead of storing the storing data (APD).

(fifth embodiment)

Next, the fifth embodiment will be described. According to this embodiment, the registration process by the issuing apparatus will be described in detail. The general outline will be described with reference to Fig.11. In this embodiment, the issuer registration apparatus 400 issues an issuer registration certificate to the issuing apparatus 100 beforehand.

First, the user apparatus sends user information (a public key, a part of a secret key and the like) to the issuing apparatus 100 in step 51. Then, the issuing apparatus 100 generates a registration certificate based on the user information, and sends the registration certificate to the user apparatus in step 52.

The card issuer may generates a registration certificate from the user information

and stores the registration certificate in a card which is provided to a user.

Next, the fifth embodiment will be described in detail with reference to Fig.12. Fig.12 shows a block diagram of the data storing system at the time of user registration.

This system includes the issuing apparatus 100, the user apparatus 300 and the issuer registration apparatus 400.

The issuer registration apparatus 400 includes a database 410 and a certificate generation part 420.

The certificate generation part 420 acquires information (PKI) used for providing certificate information from the issuing apparatus 100, generates an issuer registration certificate (IRC), stores it into the database 410, and sends it to the issuing apparatus 100.

The issuing apparatus 100 includes a database 110, a certificate generation part 120, a certificate verification part 130 and a key information generation part 150.

The certificate generation part 120 generates a registration certificate (RC) from registration information (RI) which is received from the user apparatus 300, stores the registration certificate (RC) into the database 110, and sends it to the user apparatus 300.

The certificate verification part 130 acquires the issuer registration certificate (IRC) from the issuer registration apparatus 400, and verifies the issuer registration certificate (IRC). When the issuer registration certificate (IRC) is verified, it is stored into the database 110.

The key information generation part 150 generates information (PKI) which is used for providing certificate information by the issuer.

The issuing apparatus 300 includes a memory 310, a registration information generation part 320 and a certificate verification part 330.

The registration information generation part 320 generates registration information of information (RI) (a public key, a symmetric key in symmetric key cryptography, and the like) on a key such as a user public key or a part of a secret key and stores it in the memory 310.

The certificate verification part 330 acquires the issuer registration certificate (IRC) and the registration certificate (RC) from the issuing apparatus 100 and verifies them. When both of them are verified, they are stored in the memory 110.

In the above configuration, the issuing apparatus 100 may generate the registration information (RI) instead of receiving the registration information (RI) from the issuing apparatus 100. In such a case, the issuing apparatus includes a registration information generation part.

Next, the operation of the above-mentioned configuration for user registration will be described in detail.

(1) The issuing apparatus 100 generates information (key information) used for providing certificate information (used in the certificate generation part 120) by using the key information generation part 150, and sends the information (PKI) (key information, or a part of the key information) to the issuer registration apparatus 400.

(2) The issuer registration apparatus 400 generates the issuer registration certificate (IRC) by using the information (PKI) in the certificate generation part 420. Then, the issuer registration apparatus 400 stores the information (PKI) and the

issuer registration certificate (IRC), and sends the issuer registration certificate (IRC) to the issuing apparatus 100.

The issuing apparatus 100 verifies the issuer registration certificate (IRC) in the certificate verification part 130. When it is verified, the issuer registration certificate (IRC) is stored in the database 110.

(Step 51) The user apparatus 300 generates registration information (RI) in the registration information generation part 320, stores it in the memory 310 and sends the registration information (RI) to the issuing apparatus 100. As mentioned above, the registration information (RI) can be generated by the issuing apparatus.

(Step 52) The issuing apparatus 100 generates a registration certificate (RC) by using the received registration information (RI) in the certificate generation part 120, stores the registration certificate in to the memory 110, and sends the registration certificate (RC) and the issuer registration certificate (IRC) to the user apparatus 300.

In addition, the user apparatus 300 verifies the registration certificate (RC) and the issuer registration certificate (IRC) by the certificate verification part 330. When both of them are verified, the registration certificate (RC) and the issuer registration certificate (IRC) is stored in the memory 110.

(sixth embodiment)

In the following, the general outline of the sixth embodiment will be described with reference to Fig.13. In this embodiment, a registration is issued to the data providing apparatus and a certificate is provided to application data.

As shown in Fig.13, the data registration apparatus 500 issues a registration to the data providing apparatus beforehand (the process shown in (1) and (2)).

When the user apparatus 300 sends storing data information to the data providing apparatus 200 in step 62, the data providing apparatus 200 issues a certificate of data in step 62. Then, the data providing apparatus 200 sends the data, the certificate and the data provider registration certificate to the user apparatus in step 63.

Next, this embodiment will be described in detail with reference to Fig.14. Fig.14 shows a block diagram of the data storing system for data storing according to the sixth embodiment.

This system shown in Fig.14 includes a data providing apparatus 200, the user apparatus 300 and the data registration apparatus 500.

The data registration apparatus 500 includes a database 510 and a certificate generation part 520.

The certificate generation part 520 acquires information (PKD) for providing certificate information by the data provider from the data providing apparatus 200, generates a data provider registration certificate (DPR) which is a digital signature of the data registrar to the information (PKD), stores the data provider registration certificate (DPR) in the database 510 and sends it to the data providing apparatus 200.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a key information generation part 250.

The certificate generation part 220 acquires the storing data information (SDI) from the user apparatus 300 and storing data from the

database 210. Then, the certificate generation part 220 generates storing data with a certificate (SDCI) which is the storing data (APD) and a digital signature to the storing data (APD) and the storing data information (SDI) which indicates data providing authorization. Then, the certificate generation part 220 sends the storing data (SDCI) with a certificate to the user apparatus 300.

The certificate verification part 230 acquires the data provider registration certificate (DPR) from the data registration apparatus 500 and verifies it.

The certificate verification part 330 acquires the data provider registration certificate (DPR) and the storing data with a certificate (SDCI) which is a digital signature of the data provider from the data providing apparatus 200. Then, the certificate verification part 330 verifies both of them. When they are verified, the certificate verification part 330 sends the storing data (APD) to the data verification part 340.

The data verification part 340 verifies the storing data (APD), and stored it into the memory 310 when it is verified.

The operation of the above-mentioned configuration will be described.

(1) The data registration apparatus 200 generates information (key information) used for providing certificate information (used in the certificate generation part 220) by using the key information generation part 250, and sends the information (PKD) (key information, or a part of the key information) to the data registration apparatus 500.

(2) The data registration apparatus 500 generates the data provider registration certificate (DPR) by using the information (PKD) in the

certificate generation part 520. Then, the data registration apparatus 500 stores the information (PKD) and the data provider registration certificate (DPR) in the database 510, and sends and the data provider registration certificate (DPR) to the data providing apparatus 200.

The data providing apparatus 200 verifies the data provider registration certificate (DPR) in the certificate verification part 230. When it is verified, the data provider registration certificate (DPR) is stored in the database 210.

(Step 61) The user apparatus 300 sends the storing data information (SDI) on data to be stored to the data providing apparatus 200.

(Step 62, 63) The data providing apparatus 200 acquires necessary data information (APD) from the database 210 by using the received storing information. Then, the data providing apparatus 200 generates the storing data with a certificate (SDCI) which is on the storing data information (SDI) and the storing data (APD) and sends the storing data with the certificate (SDCI) and the data provider registration certificate (DPR) to the user apparatus 300.

The user apparatus 300 verifies the storing data with the certificate (SDCI) and the data provider registration certificate (DPR) in the certificate verification part 330. When both of them are verified, the storing data (APD) which is extracted from the storing data with the certificate (SDCI) is sent to the data verification part 340. Then, the data verification part 340 verifies that the storing data (APD) corresponds to the requested storing data information (SDI). When it is verified, the storing data (APD) is stored in the memory 310.

(seventh embodiment)

In the above-mentioned sixth embodiment,

the data registration apparatus 500 may generate the storing data with the certificate (SDCI). In the following, the operation in this case will be described with reference to Fig.15 as a seventh embodiment. The configuration shown in Fig.15 does not includes the certificate generation part 220 and the key information generation part 250, instead, includes a storing data acquisition part 250.

First, the data providing apparatus 200 acquire the storing data (APD), which is stored by a user, from the database 210 by using the storing data information (SDI) as a key.

Next, the data providing apparatus 200 sends the storing data (APD) and information on the storing data (APD) (the storing data information (SDI), the size of the storing data (APD) or the like) to the data registration apparatus 500.

The data registration apparatus 500 generates a data certificate (SDCI') from the storing data (APD) and the information by using the certificate generation part 520, and stores the storing data (APD) and the data certificate (SDCI') in the database 510. Then, the data registration apparatus 500 sends the data certificate (SDCI') in the database 210.

The user apparatus 300 sends the storing data information (SDI), which is information on data to be stored, to the data providing apparatus 200.

The data providing apparatus 200 acquires data (SDCI) which includes the necessary storing data (APD), the data certificate (SDCI') and the information on the storing data (APD) from the database 210 by using the received storing data information (SDI), and sends the data (SDCI) to the user apparatus 300.

The user apparatus 300 verifies the data (SDCI) by using the certificate verification part

330. When the data (SDCI) is verified, the storing data extracted from the data (SDCI) is sent to the data verification part 340. The verification part 340 verifies that requested data corresponds to the extracted storing data (APD). When it is verified, the storing data (APD) is stored in the memory 310.

The above-mentioned embodiments is described on the basis of each element shown in each figure. In addition, each element in the user apparatus, the data providing apparatus, the data registration apparatus, the issuing apparatus and issuer registration apparatus can be constructed by a program. The program can be stored in a disk device which is connected to a computer which can be used as the user apparatus, the data providing apparatus, the data registration apparatus, the issuing apparatus or the issuer registration apparatus. In addition, the program can be stored in a transportable recording medium such as a floppy disk, CD-ROM and the like. By installing the program stored in these medium to a computer, the present invention can be realized.

The computer system which can be used the issuing apparatus, the data providing apparatus and the like may be configured as shown in Fig.15 for example. The computer system includes a CPU 600 which executes processes, a memory 601 which stores programs and data, a hard disk 602 which stores programs and data used in the memory 601 or the CPU 600, a display 603 which displays data, a keyboard 604 for inputting data or commands and a communication processing apparatus 605 which performs communication with another computer via a network. By installing a program which executes processes of the issuing apparatus and the data providing apparatus and the like which are described in detail in each embodiment, the computer can be

used as the issuing apparatus, the data providing apparatus and the like. The program is installed in the memory 601 or the hard disk 602, and executed by the CPU 600.

As mentioned above, according to the present invention, the following effects can be obtained.

(1) By the registration certificate which is issued by the registration issuer, the party which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

That is, since the public key information used for a certificate is certified by the registration issued by each registrar, the validity of the authorization is insured such that both of the card issuer and the service provider perform processes safely. In addition, since the issuer which is certified issues the registration certificate of a card, the validity of the card is insured.

(2) By mutual agreement between the user, the card issuer and the service provider, the card issuer and the service provider equally can store and delete data in a card safely.

That is, as mentioned above, since a party issues the storing authorization to another party which performs data download, data download is not performed only by one of the card issuer and the service provider without authorization by another party such that data can be stored and deleted safely.

(3) Each of the card issuer and the service provider can obtain information on data which is stored an IC card.

That is, since data download is performed

after each of the user, the card issuer and the service provider reaches an agreement, each of the card issuer and the service provider can obtain information on an application and a card which stores the application.

In the future, as the number of applications which are downloaded in IC cards increases, it becomes important to obtain the above-mentioned information.

In addition, according to the present invention, a service provider can store data to a card which is issued by any IC card issuer safely.

The present invention is not limited to the specifically disclosed embodiments, and variations and modifications may be made without departing from the scope of the invention.

WHAT IS CLAIMED IS:

1. A data storing system comprising:

a user apparatus which stores data;

an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

a data providing apparatus which is held by a data provider that provides data;

an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and

a data registration apparatus which is held by a data registrar that registers and manages the data provider;

wherein the user apparatus comprises:

registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus.

2. A data storing system comprising:

a user apparatus which stores data;

an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

a data providing apparatus which is held by a data provider that provides data;

an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and

a data registration apparatus which is held by a data registrar that registers and manages the data provider;

wherein the user apparatus comprises:

registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for registration information and user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises:

registration information generation means which generates registration information on a key including a user public key or a part of a secret key and generates user information;

registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus.

3. The data storing system as claimed in claim 1, the user apparatus further comprising:

means which sends the registration certificate and storing data information to the issuing apparatus;

means which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

means which verifies that the storing data information corresponds to storing data which is acquired; and

means which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

the issuing apparatus further comprising:

means which verifies the registration certificate and the storing data information which are received from the user apparatus;

means which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

means which verifies a storing authorization which is received from the data providing apparatus; and

means which sends the storing authorization to the user apparatus when the storing authorization is verified;

the data providing apparatus further comprising:

means which verifies the storing authorization request;

means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

4. The data storing system as claimed in claim 1, the user apparatus further comprising:

means which sends the registration certificate and storing data information to the data providing apparatus;

means which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

means which verifies that the storing data information corresponds to storing data which is acquired; and

means which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

the data providing apparatus further comprising:

means which verifies the registration certificate and the storing data information which are received from the user apparatus;

means which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are

verified; and

means which sends the registration certificate, the storing data information and the storing authorization request to the issuing apparatus;

means which verifies a storing authorization which is received from the issuing apparatus; and

means which sends the storing authorization to the user apparatus when the storing authorization is verified;

the issuing apparatus further comprising:

means which verifies the storing authorization request;

means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the data providing apparatus.

5. The data storing system as claimed in claim 1, the user apparatus further comprising:

means which sends the registration certificate and storing data information to the data providing apparatus;

means which verifies a storing authorization which is received from the data providing apparatus;

means which verifies that the storing data information corresponds to storing data which is acquired;

means which stores the storing data in the storage device when it is verified that the storing

data information corresponds to the storing data;

the data providing apparatus further comprising:

means which verifies the registration certificate which is received from the user apparatus;

means which generates a storing authorization wherein certificate information is provided to the registration certificate and the storing data information when the registration certificate is verified, and sends the storing authorization to the user apparatus.

6. The data storing system as claimed in claim 1, the issuing apparatus further comprising:

means which sends information used for providing certificate information to the issuer registration apparatus;

means which verifies an issuer registration certificate which is received from the issuer registration apparatus;

means which stores the issuer registration certificate when the issuer registration certificate is verified;

means which generates the registration certificate to the user apparatus, and sends the registration certificate to the user apparatus with the issuer registration certificate;

the issuer registration apparatus further comprising:

means which provides certificate information to the information used for providing the certificate information for generating the issuer registration certificate, and sends the

issuer registration certificate to the issuing apparatus;

the user apparatus further comprising:

means which verifies the registration certificate and the issuer registration certificate which are received from the issuing apparatus; and

means which stores the registration certificate and the issuer registration certificate into the storage device when the registration certificate and the issuer registration certificate are verified.

7. The data storing system as claimed in claim 3, the data providing apparatus further comprising:

means which sends information used for providing certificate information to the data registration apparatus;

means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

the data registration apparatus further comprising;

means which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and

sends the data provider registration certificate to the data providing apparatus;

the user apparatus further comprising;

means which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

8. The data storing system as claimed in claim 4, the data providing apparatus further comprising:

means which sends information used for providing certificate information to the data registration apparatus;

means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

the data registration apparatus further comprising;

means which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

the user apparatus further comprising;

means which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

9. The data storing system as claimed in claim 5, the data providing apparatus further comprising:

means which sends information used for providing certificate information to the data registration apparatus;

means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

the data registration apparatus further comprising;

means which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

the user apparatus further comprising;

means which verifies the storing data with

certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

10. The data storing system as claimed in claim 3, the data providing apparatus further comprising:

means which sends storing data to be stored in the user apparatus and information used for providing certificate information to the data registration apparatus;

the data registration apparatus further comprising;

means which generates data certificate wherein certificate information is added to the storing information and the information which is received from the data providing apparatus, and sends the data certificate to the data providing apparatus;

the data providing apparatus further comprising:

means which verifies the data certificate received from the data registration apparatus, and stores the data certificate when the data certificate is verified;

means which sends the storing data and the data certificate as storing data with certificate information to the user apparatus;

the user apparatus further comprising;

means which receives and verifies the storing data with certificate information, and stores the storing data into the storage device when

the storing data with certificate information is verified.

11. The data storing system as claimed in claim 3, the user apparatus further comprising means which deletes the storing data which is in the storage device.

12. The data storing system as claimed in claim 4, the user apparatus further comprising means which deletes the storing data which is in the storage device.

13. The data storing system as claimed in claim 5, the user apparatus further comprising means which deletes the storing data which is in the storage device.

14. An issuing apparatus in a data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration

apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising:

means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

15. An issuing apparatus in a data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising:

means which generates user information and registration information on a key including a user public key or a part of a secret key; and

registration generation means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user

apparatus.

16. The issuing apparatus as claimed in claim 14, further comprising:

means which receives the registration certificate and storing data information from the user apparatus;

means which verifies the registration certificate and the storing data information;

means which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

means which verifies a storing authorization which is received from the data providing apparatus; and

means which sends the storing authorization to the user apparatus when the storing authorization is verified.

17. The issuing apparatus as claimed in claim 14, further comprising:

means which receives the registration certificate, storing data information and a storing authorization request from the data providing

apparatus;

means which verifies the storing authorization request;

means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the data providing apparatus.

18. The issuing apparatus as claimed in claim 14, further comprising:

means which sends information used for providing certificate information to the issuer registration apparatus;

means which verifies an issuer registration certificate which is received from the issuer registration apparatus;

means which stores the issuer registration certificate when the issuer registration certificate is verified;

means which generates the registration certificate to the user apparatus, and sends the registration certificate to the user apparatus with the issuer registration certificate.

19. A data providing apparatus in data storing system which comprises: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

the data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises:

registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus,

the data providing apparatus comprising:

means which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

means which verifies the storing authorization request;

means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

20. The data providing apparatus as claimed in claim 19, further comprising:

means which verifies the registration certificate and storing data information which are received from the user apparatus;

means which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

means which sends the registration certificate, the storing data information and the storing authorization request to the issuing apparatus;

means which verifies a storing authorization which is received from the issuing apparatus; and

means which sends the storing authorization to the user apparatus when the storing authorization is verified.

21. The data providing apparatus as claimed in claim 19, further comprising:

means which receives the registration certificate and storing data information from the user apparatus;

means which verifies the registration certificate;

means which generates a storing authorization wherein certificate information is

provided to the registration certificate and the storing data information when the registration certificate is verified, and sends the storing authorization to the user apparatus.

22. The data providing apparatus as claimed in claim 19, further comprising:

means which sends information used for providing certificate information to the data registration apparatus;

means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information; and

means which sends the data provider registration certificate and the storing data with certificate information to the user apparatus.

23. A computer readable medium storing program code for causing a data storing system to store data, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus

which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider; the computer readable medium comprising:

registration information generation program code means, provided for the user apparatus, which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and

registration verification program code means, provided for the user apparatus, which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

registration generation program code means, provided for the issuing apparatus, which generates the registration certificate and sends the registration certificate to the user apparatus.

24. A computer readable medium storing program code for causing a data storing system to store data, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus

which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider; the computer readable medium comprising:

registration verification program code means, provided for the user apparatus, which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for registration information and user information, stores the registration certificate to a storage device when the registration certificate is verified;

registration information generation program code means, provided for the issuing apparatus, which generates registration information on a key including a user public key or a part of a secret key and generates user information;

registration generation program code means, provided for the issuing apparatus, which generates the registration certificate and sends the registration certificate to the user apparatus.

25. The computer readable medium as claimed in claim 23, further comprising:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the issuing apparatus;

program code means, provided for the user apparatus, which verifies a storing authorization

when the storing authorization is received from the issuing apparatus;

program code means, provided for the user apparatus, which verifies that the storing data information corresponds to storing data which is acquired; and

program code means, provided for the user apparatus, which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

program code means, provided for the issuing apparatus, which verifies the registration certificate and the storing data information which are received from the user apparatus;

program code means, provided for the issuing apparatus, which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

program code means, provided for the issuing apparatus, which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

program code means, provided for the issuing apparatus, which verifies a storing authorization which is received from the data providing apparatus; and

program code means, provided for the issuing apparatus, which sends the storing authorization to the user apparatus when the storing authorization is verified;

program code means, provided for the data providing apparatus, which verifies the storing authorization request;

program code means, provided for the data providing apparatus, which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

26. The computer readable medium as claimed in claim 23, further comprising:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the data providing apparatus;

program code means, provided for the user apparatus, which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

program code means, provided for the user apparatus, which verifies that the storing data information corresponds to storing data which is acquired; and

program code means, provided for the user apparatus, which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

program code means, provided for the data providing apparatus, which verifies the registration certificate and the storing data information which are received from the user apparatus;

program code means, provided for the data providing apparatus, which provides certificate information to the registration certificate and the storing data information for generating a storing

authorization request when the registration certificate and the storing data information are verified; and

program code means, provided for the data providing apparatus, which sends the registration certificate, the storing data information and the storing authorization request to the issuing apparatus;

program code means, provided for the data providing apparatus, which verifies a storing authorization which is received from the issuing apparatus; and

program code means, provided for the data providing apparatus, which sends the storing authorization to the user apparatus when the storing authorization is verified;

program code means, provided for the issuing apparatus, which verifies the storing authorization request;

program code means, provided for the issuing apparatus, which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the data providing apparatus.

27. The computer readable medium as claimed in claim 23, further comprising:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the data providing apparatus;

program code means, provided for the user

apparatus, which verifies a storing authorization which is received from the data providing apparatus;

program code means, provided for the user apparatus, which verifies that the storing data information corresponds to storing data which is acquired;

program code means, provided for the user apparatus, which stores the storing data in the storage device when it is verified that the storing data information corresponds to the storing data;

program code means, provided for the data providing apparatus, which verifies the registration certificate which is received from the user apparatus;

program code means, provided for the data providing apparatus, which generates a storing authorization wherein certificate information is provided to the registration certificate and the storing data information when the registration certificate is verified, and sends the storing authorization to the user apparatus.

28. The computer readable medium as claimed in claim 23, further comprising:

program code means, provided for the issuing apparatus, which sends information used for providing certificate information to the issuer registration apparatus;

program code means, provided for the issuing apparatus, which verifies an issuer registration certificate which is received from the issuer registration apparatus;

program code means, provided for the issuing apparatus, which stores the issuer

registration certificate when the issuer registration certificate is verified;

program code means, provided for the issuing apparatus, which generates the registration certificate to the user apparatus, and sends the registration certificate to the user apparatus with the issuer registration certificate;

program code means, provided for the issuer registration apparatus, which provides certificate information to the information used for providing the certificate information for generating the issuer registration certificate, and sends the issuer registration certificate to the issuing apparatus;

program code means, provided for the user apparatus, which verifies the registration certificate and the issuer registration certificate which are received from the issuing apparatus; and

program code means, provided for the user apparatus, which stores the registration certificate and the issuer registration certificate into the storage device when the registration certificate and the issuer registration certificate are verified.

29. The computer readable medium as claimed in claim 25, further comprising:

program code means, provided for the data providing apparatus, which sends information used for providing certificate information to the data registration apparatus;

program code means, provided for the data providing apparatus, which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider

registration certificate when the data provider registration certificate is verified;

program code means, provided for the data providing apparatus, which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

program code means, provided for the data registration apparatus, which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

program code means, provided for the user apparatus, which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

30. The computer readable medium as claimed in claim 26, further comprising:

program code means, provided for the data providing apparatus, which sends information used for providing certificate information to the data registration apparatus;

program code means, provided for the data providing apparatus, which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider

registration certificate is verified;

program code means, provided for the data providing apparatus, which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

program code means, provided for the data registration apparatus, which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

program code means, provided for the user apparatus, which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

31. The computer readable medium as claimed in claim 27, further comprising:

program code means, provided for the data providing apparatus, which sends information used for providing certificate information to the data registration apparatus;

program code means, provided for the data providing apparatus, which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

program code means, provided for the data providing apparatus, which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

program code means, provided for the data registration apparatus, which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

program code means, provided for the user apparatus, which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

32. The computer readable medium as claimed in claim 25, further comprising:

program code means, provided for the data providing apparatus, which sends storing data to be stored in the user apparatus and information used for providing certificate information to the data registration apparatus;

program code means, provided for the data registration apparatus, which generates data certificate wherein certificate information is added to the storing information and the information which is received from the data providing apparatus, and sends the data certificate to the data providing

apparatus;

program code means, provided for the data providing apparatus, which verifies the data certificate received from the data registration apparatus, and stores the data certificate when the data certificate is verified;

program code means, provided for the data providing apparatus, which sends the storing data and the data certificate as storing data with certificate information to the user apparatus;

program code means, provided for the user apparatus, which receives and verifies the storing data with certificate information, and stores the storing data into the storage device when the storing data with certificate information is verified.

33. The computer readable medium as claimed in claim 25, further comprising:

program code means, provided for the user apparatus, which deletes the storing data which is in the storage device.

34. The computer readable medium as claimed in claim 26, further comprising:

program code means, provided for the user apparatus, which deletes the storing data which is in the storage device.

35. The computer readable medium as claimed in claim 27, further comprising:

program code means, provided for the user apparatus, which deletes the storing data which is in the storage device.

36. A computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising:

program code means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation program code means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

37. A computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising:

program code means which generates user information and registration information on a key including a user public key or a part of a secret key; and

registration generation program code means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

38. The computer readable medium as claimed in claim 36, further comprising:

program code means which receives the registration certificate and storing data information from the user apparatus;

program code means which verifies the registration certificate and the storing data information;

program code means which provides certificate information to the registration

certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

program code means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

program code means which verifies a storing authorization which is received from the data providing apparatus; and

program code means which sends the storing authorization to the user apparatus when the storing authorization is verified.

39. The computer readable medium as claimed in claim 36, further comprising:

program code means which receives the registration certificate, storing data information and a storing authorization request from the data providing apparatus;

program code means which verifies the storing authorization request;

program code means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the data providing apparatus.

40. The computer readable medium as claimed in claim 36, further comprising:

program code means which sends information used for providing certificate information to the issuer registration apparatus;

program code means which verifies an issuer registration certificate which is received from the issuer registration apparatus;

program code means which stores the issuer registration certificate when the issuer registration certificate is verified;

program code means which generates the registration certificate to the user apparatus, and sends the registration certificate to the user apparatus with the issuer registration certificate.

41. A computer readable medium storing program code for causing a data providing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises:

registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the

issuing apparatus with user information; and

registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified;

wherein the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus,

the computer readable medium comprising:

program code means which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

program code means which verifies the storing authorization request;

program code means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

42. The computer readable medium as claimed in claim 41, further comprising:

program code means which verifies the registration certificate and storing data information which are received from the user apparatus;

program code means which provides

certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

program code means which sends the registration certificate, the storing data information and the storing authorization request to the issuing apparatus;

program code means which verifies a storing authorization which is received from the issuing apparatus; and

program code means which sends the storing authorization to the user apparatus when the storing authorization is verified.

43. The computer readable medium as claimed in claim 41, further comprising:

program code means which receives the registration certificate and storing data information from the user apparatus;

program code means which verifies the registration certificate;

program code means which generates a storing authorization wherein certificate information is provided to the registration certificate and the storing data information when the registration certificate is verified, and sends the storing authorization to the user apparatus.

44. The computer readable medium as

claimed in claim 41, further comprising:

program code means which sends information used for providing certificate information to the data registration apparatus;

program code means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

program code means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information; and

program code means which sends the data provider registration certificate and the storing data with certificate information to the user apparatus.

ABSTRACT OF THE DISCLOSURE

A data storing system is provided, wherein the data storing system includes: a user apparatus; an issuing apparatus which issues a registration certificate; a data providing apparatus; an issuer registration apparatus; and a data registration apparatus; wherein the user apparatus includes: a part which generates registration information on a key including a user public key, sends the registration information to the issuing apparatus with user information; and a part which verifies a registration certificate, received from the issuing apparatus, which is signature information of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified; wherein the issuing apparatus includes a part which generates the registration certificate and sends the registration certificate to the user apparatus.

FIG. 1

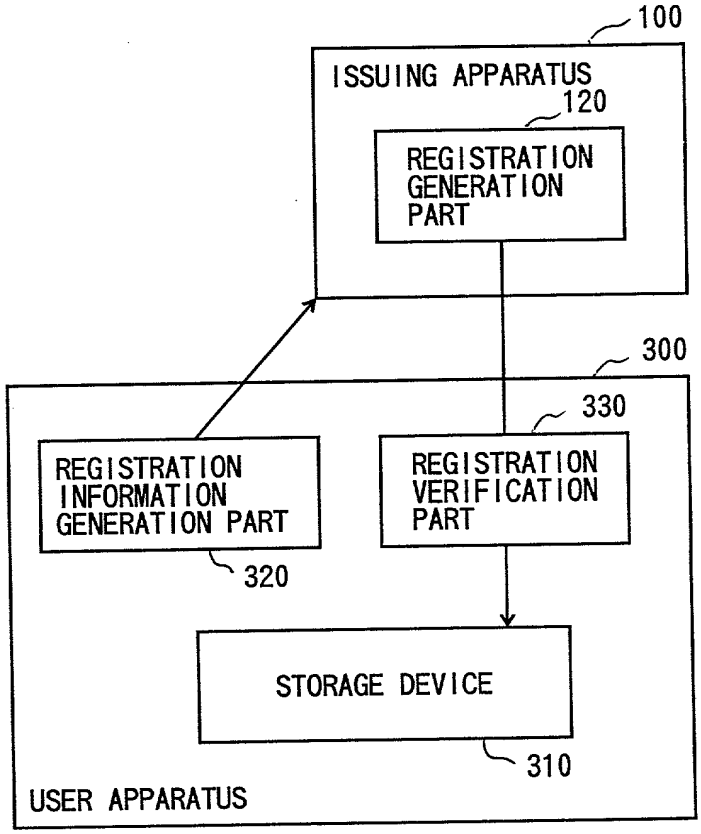

100
ISSUING APPARATUS
120
REGISTRATION GENERATION PART
300
330
REGISTRATION INFORMATION GENERATION PART
320
REGISTRATION VERIFICATION PART
STORAGE DEVICE
310
USER APPARATUS

FIG. 2

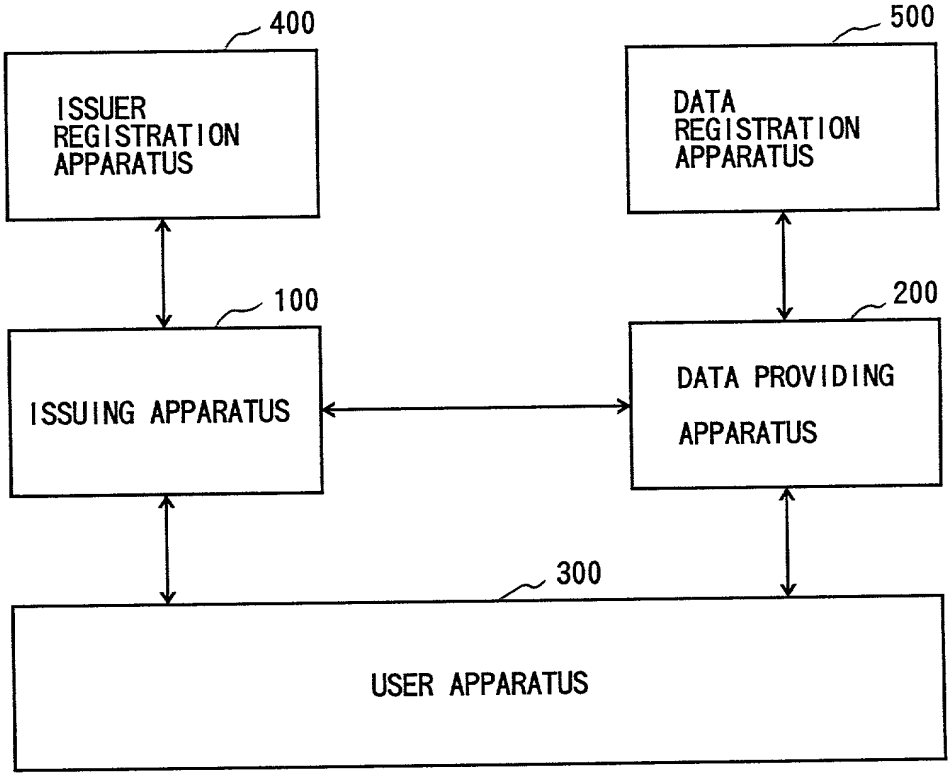

400
ISSUER REGISTRATION APPARATUS
500
DATA REGISTRATION APPARATUS
100
ISSUING APPARATUS
200
DATA PROVIDING APPARATUS
300
USER APPARATUS

FIG. 3

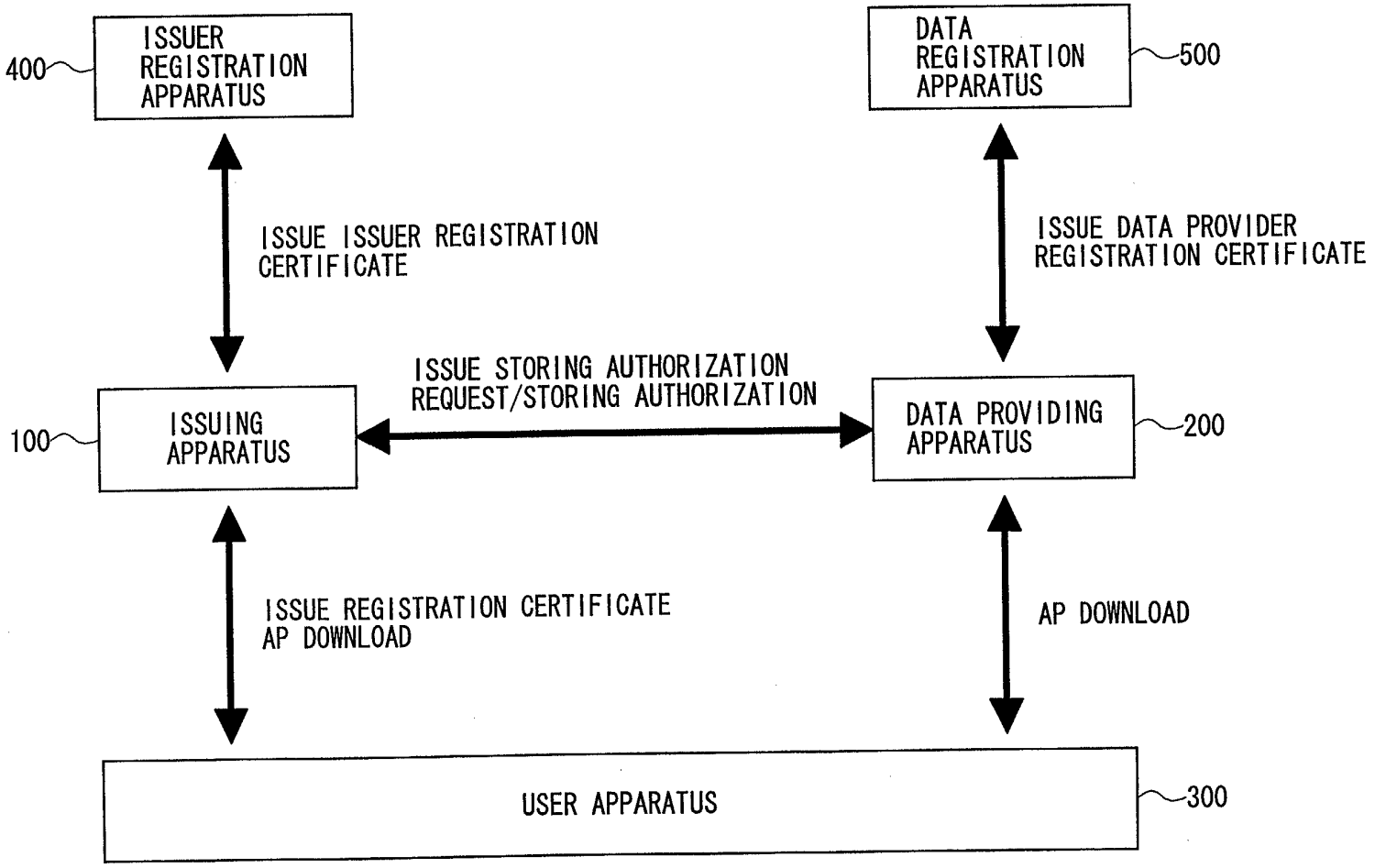

ISSUER REGISTRATION APPARATUS
400
DATA REGISTRATION APPARATUS
500
ISSUE ISSUER REGISTRATION CERTIFICATE
ISSUE DATA PROVIDER REGISTRATION CERTIFICATE
ISSUE STORING AUTHORIZATION REQUEST/STORING AUTHORIZATION
ISSUING APPARATUS
100
DATA PROVIDING APPARATUS
200
ISSUE REGISTRATION CERTIFICATE AP DOWNLOAD
AP DOWNLOAD
USER APPARATUS
300

FIG. 4

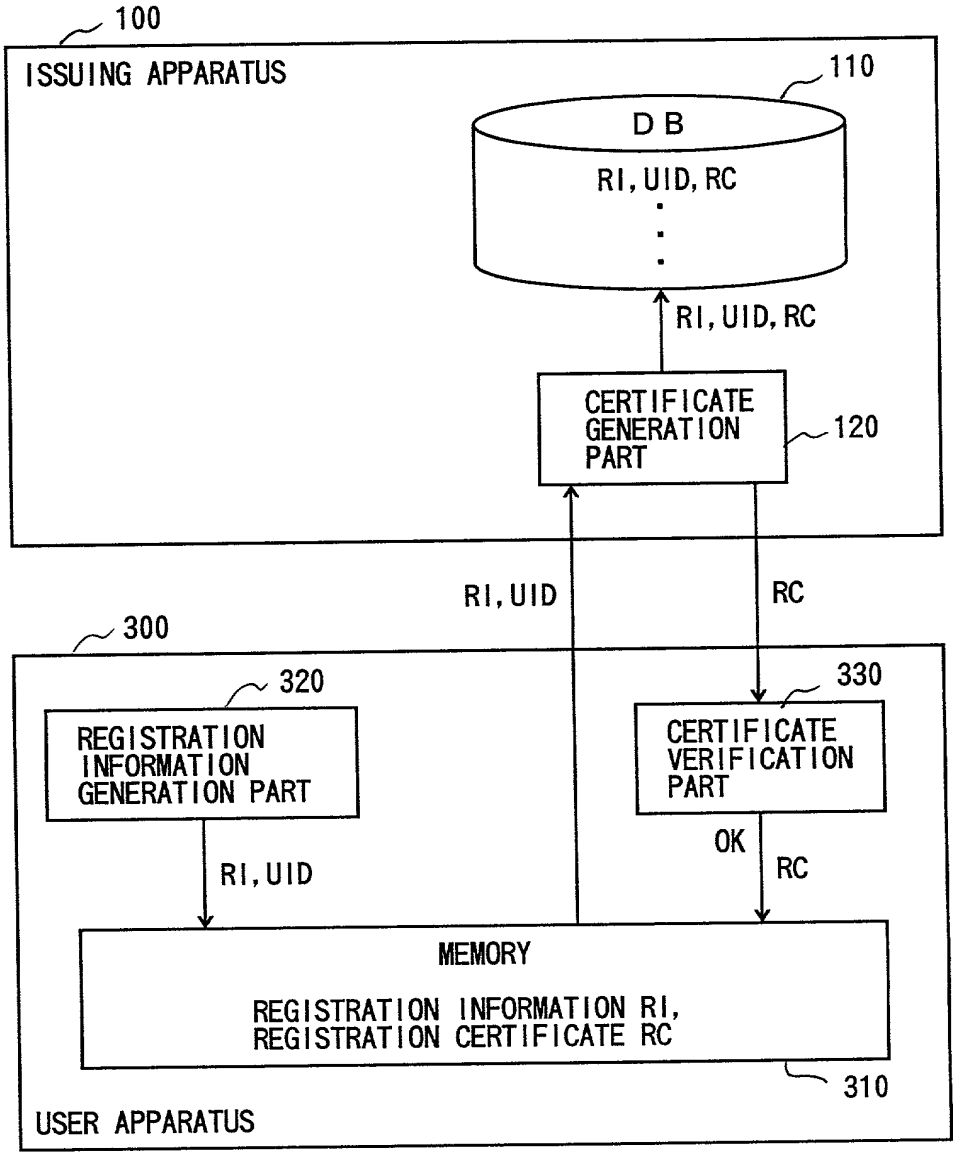

100
ISSUING APPARATUS
110
DB
RI, UID, RC
RI, UID, RC
CERTIFICATE GENERATION PART
120
RI, UID
RC
300
320
REGISTRATION INFORMATION GENERATION PART
330
CERTIFICATE VERIFICATION PART
OK
RC
RI, UID
MEMORY
REGISTRATION INFORMATION RI,
REGISTRATION CERTIFICATE RC
310
USER APPARATUS

FIG. 5

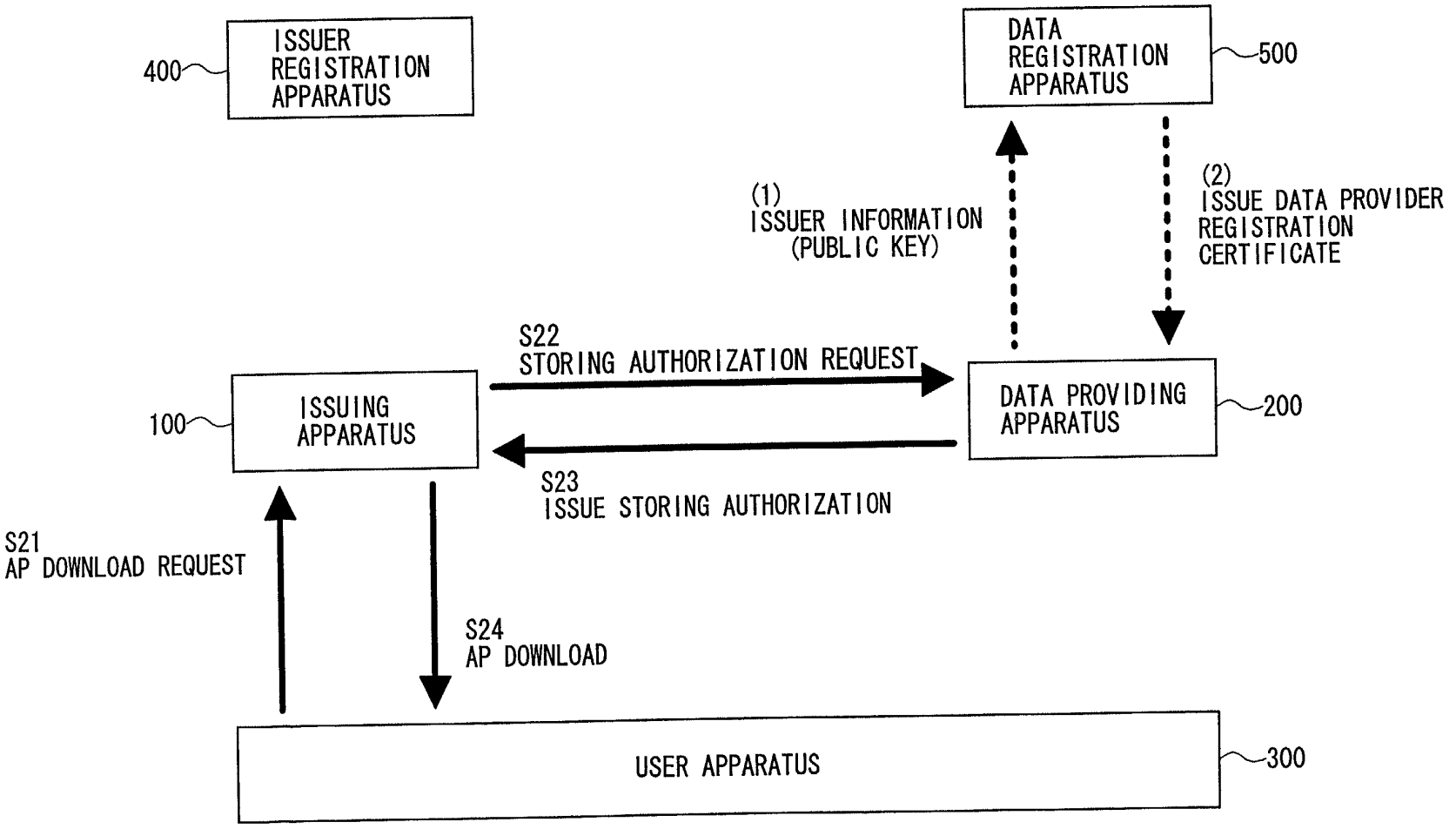

400
ISSUER REGISTRATION APPARATUS
DATA REGISTRATION APPARATUS
500
(1) ISSUER INFORMATION (PUBLIC KEY)
(2) ISSUE DATA PROVIDER REGISTRATION CERTIFICATE
S22 STORING AUTHORIZATION REQUEST
100
ISSUING APPARATUS
DATA PROVIDING APPARATUS
200
S23 ISSUE STORING AUTHORIZATION
S21 AP DOWNLOAD REQUEST
S24 AP DOWNLOAD
USER APPARATUS
300

FIG. 6

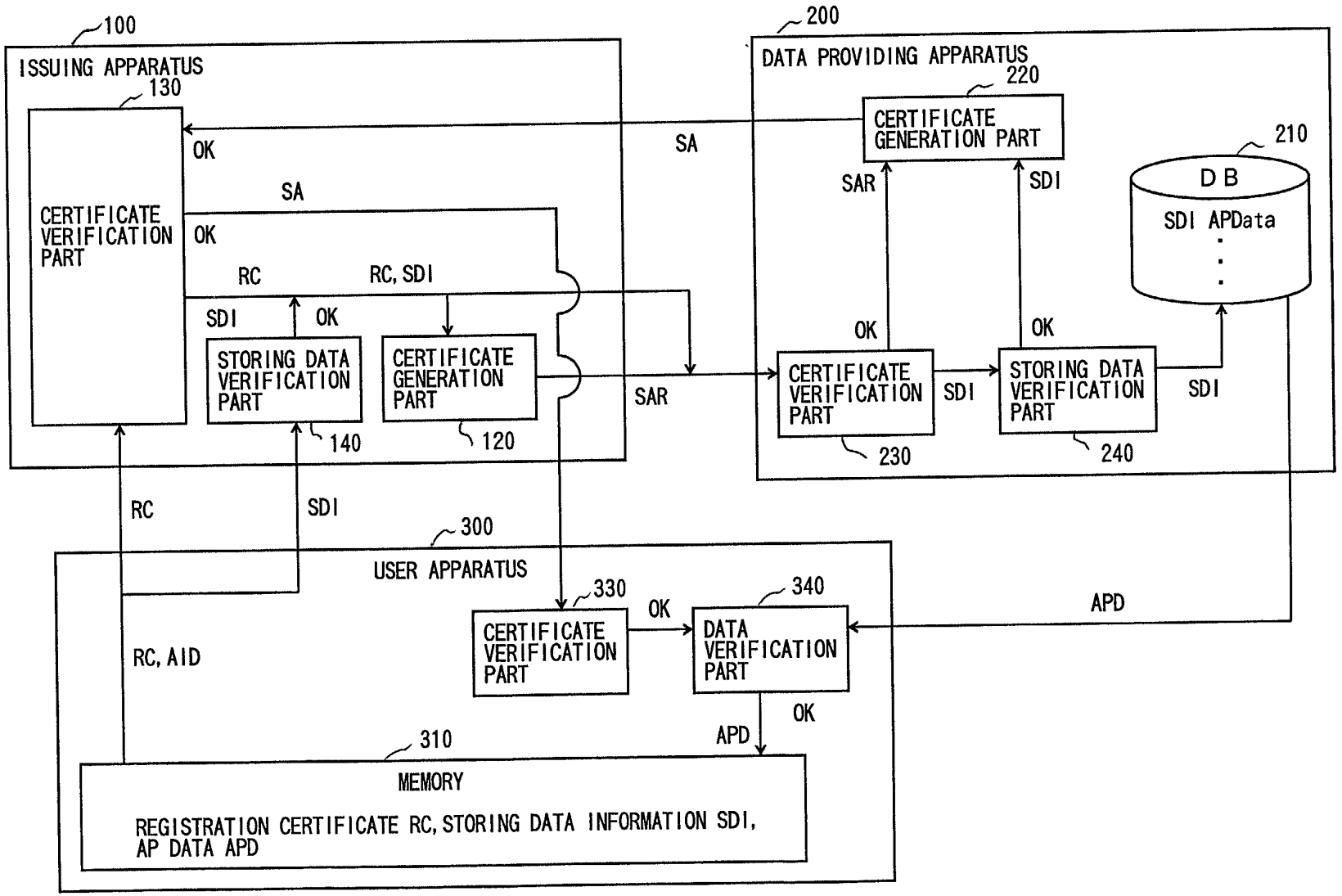

100
ISSUING APPARATUS
130
CERTIFICATE VERIFICATION PART
OK
SA
OK
RC
RC, SDI
SDI
OK
STORING DATA VERIFICATION PART
140
CERTIFICATE GENERATION PART
120
SAR
200
DATA PROVIDING APPARATUS
220
CERTIFICATE GENERATION PART
SA
SAR
SDI
210
DB
SDI APData
OK
OK
CERTIFICATE VERIFICATION PART
230
SDI
STORING DATA VERIFICATION PART
240
SDI
RC
SDI
300
USER APPARATUS
330
CERTIFICATE VERIFICATION PART
OK
340
DATA VERIFICATION PART
APD
RC, AID
OK
APD
310
MEMORY
REGISTRATION CERTIFICATE RC, STORING DATA INFORMATION SDI, AP DATA APD

FIG. 7

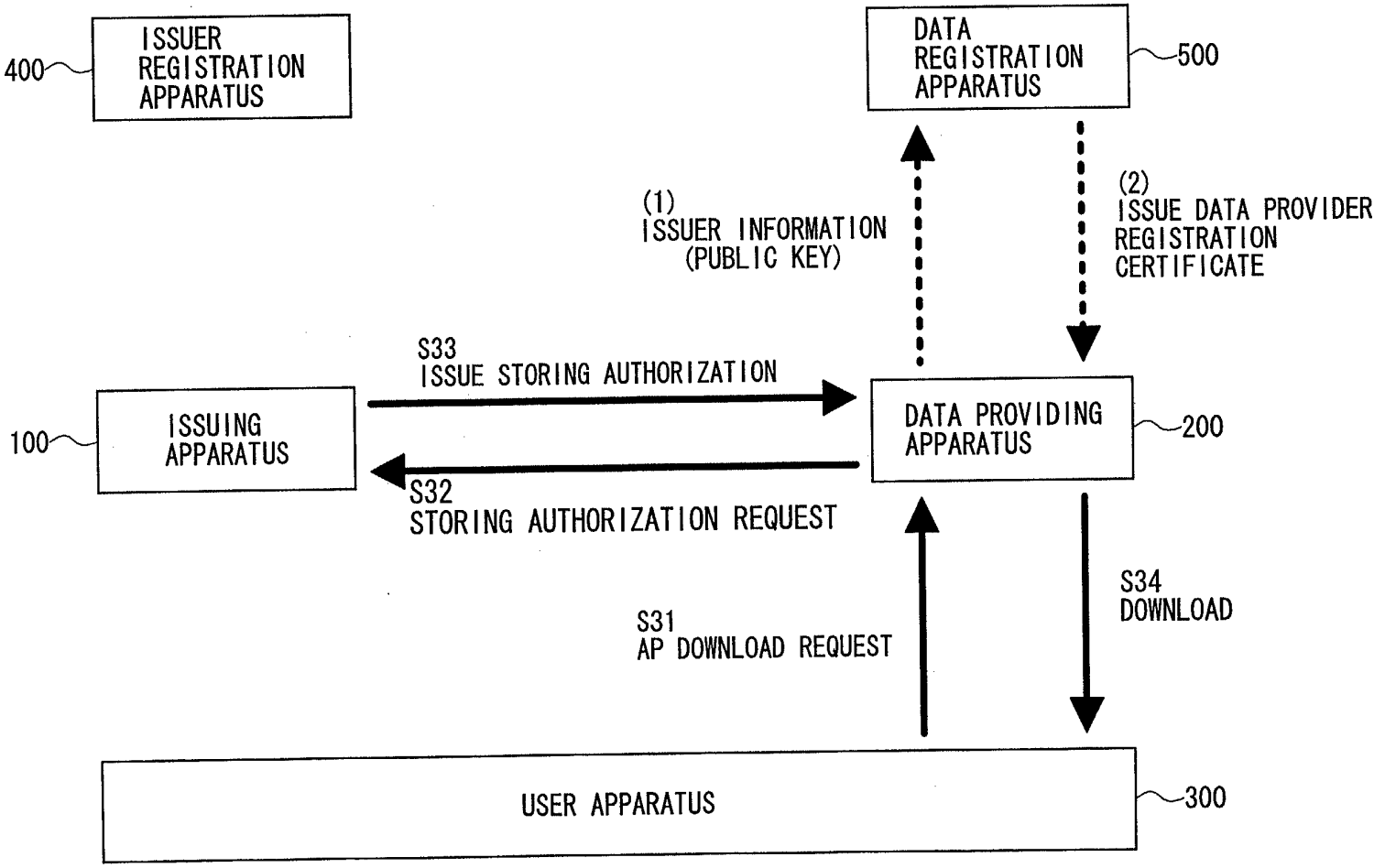

ISSUER REGISTRATION APPARATUS
400
DATA REGISTRATION APPARATUS
500
(1) ISSUER INFORMATION (PUBLIC KEY)
(2) ISSUE DATA PROVIDER REGISTRATION CERTIFICATE
S33 ISSUE STORING AUTHORIZATION
ISSUING APPARATUS
100
DATA PROVIDING APPARATUS
200
S32 STORING AUTHORIZATION REQUEST
S34 DOWNLOAD
S31 AP DOWNLOAD REQUEST
USER APPARATUS
300

FIG. 8

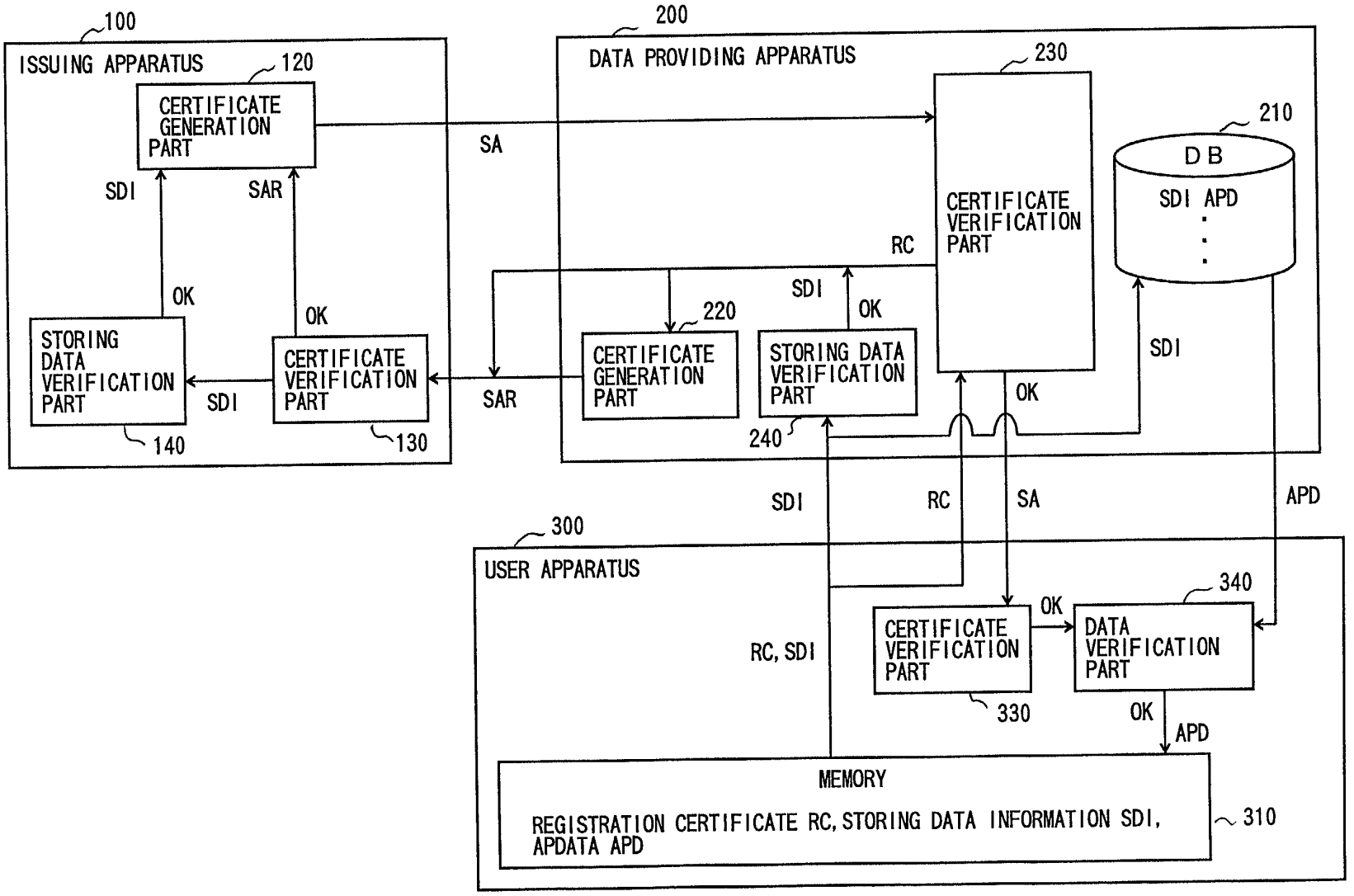

100
ISSUING APPARATUS
120
CERTIFICATE GENERATION PART
SDI
SAR
OK
OK
STORING DATA VERIFICATION PART
SDI
CERTIFICATE VERIFICATION PART
140
130
SA
SAR
200
DATA PROVIDING APPARATUS
230
CERTIFICATE VERIFICATION PART
210
DB
SDI APD
RC
SDI
OK
220
CERTIFICATE GENERATION PART
STORING DATA VERIFICATION PART
240
OK
SDI
SDI
RC
SA
APD
300
USER APPARATUS
340
OK
CERTIFICATE VERIFICATION PART
DATA VERIFICATION PART
RC, SDI
330
OK
APD
MEMORY
REGISTRATION CERTIFICATE RC, STORING DATA INFORMATION SDI, APDATA APD
310

FIG. 9

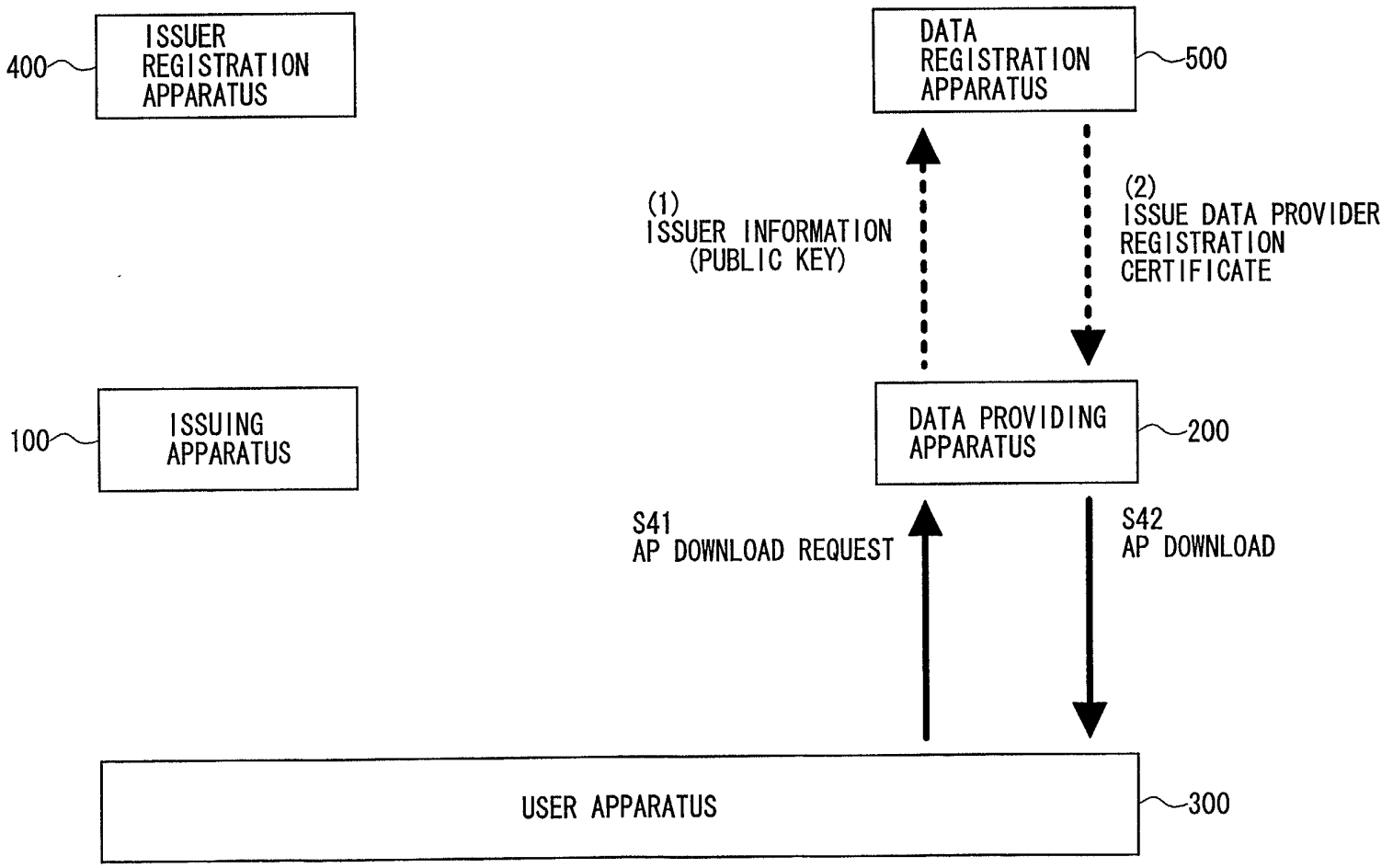

400
ISSUER REGISTRATION APPARATUS
DATA REGISTRATION APPARATUS
500
(1) ISSUER INFORMATION (PUBLIC KEY)
(2) ISSUE DATA PROVIDER REGISTRATION CERTIFICATE
100
ISSUING APPARATUS
DATA PROVIDING APPARATUS
200
S41 AP DOWNLOAD REQUEST
S42 AP DOWNLOAD
USER APPARATUS
300

FIG. 10

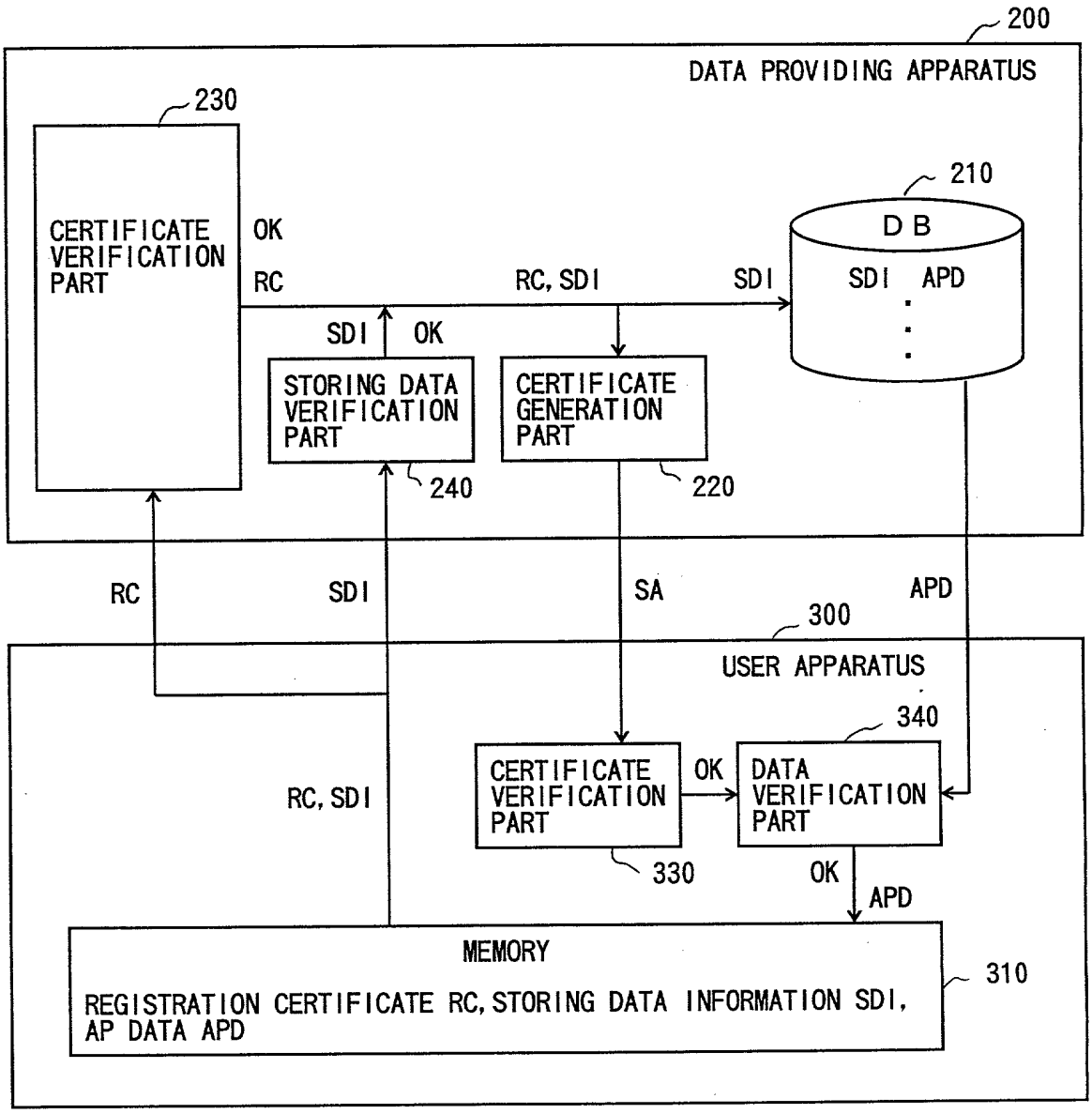

200
DATA PROVIDING APPARATUS
230
CERTIFICATE VERIFICATION PART
OK
RC
RC, SDI
SDI
210
D B
SDI APD
SDI
OK
STORING DATA VERIFICATION PART
240
CERTIFICATE GENERATION PART
220
RC
SDI
SA
APD
300
USER APPARATUS
340
CERTIFICATE VERIFICATION PART
OK
DATA VERIFICATION PART
RC, SDI
330
OK
APD
MEMORY
REGISTRATION CERTIFICATE RC, STORING DATA INFORMATION SDI, AP DATA APD
310

FIG. 11

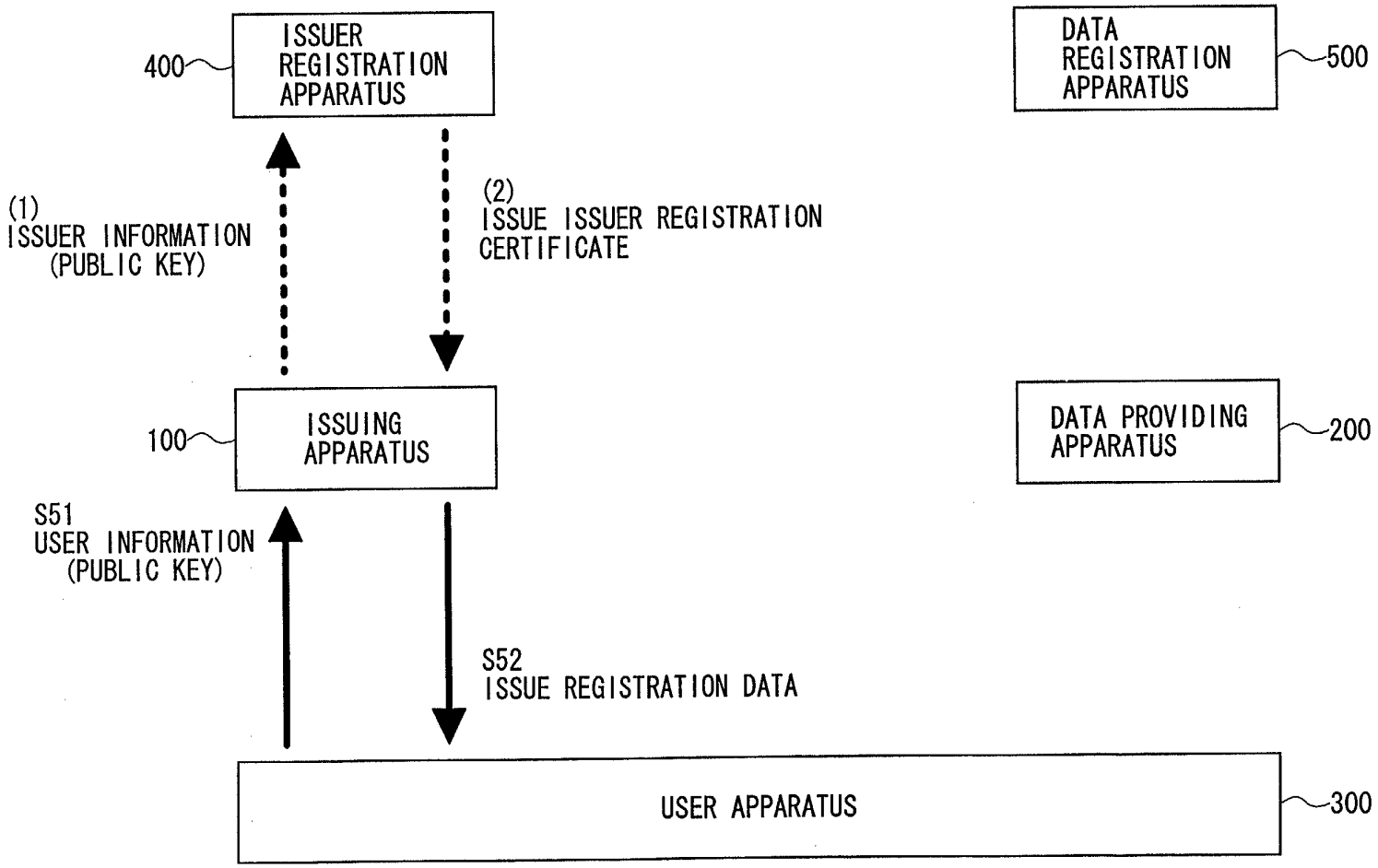

400
ISSUER REGISTRATION APPARATUS
DATA REGISTRATION APPARATUS
500
(1)
ISSUER INFORMATION (PUBLIC KEY)
(2)
ISSUE ISSUER REGISTRATION CERTIFICATE
100
ISSUING APPARATUS
DATA PROVIDING APPARATUS
200
S51
USER INFORMATION (PUBLIC KEY)
S52
ISSUE REGISTRATION DATA
USER APPARATUS
300

FIG. 12

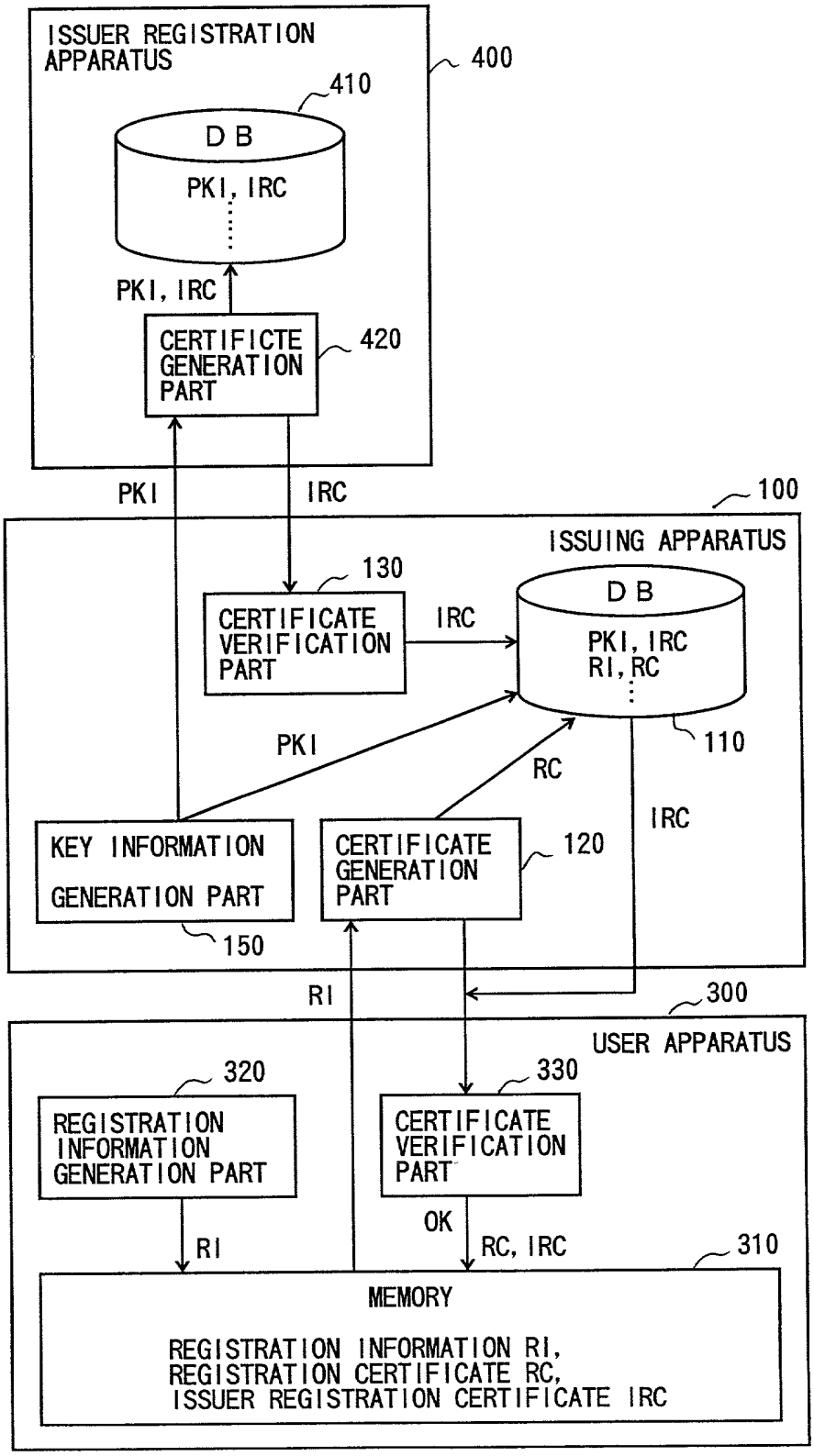

ISSUER REGISTRATION APPARATUS
400
410
D B
PKI, IRC
PKI, IRC
CERTIFICTE GENERATION PART
420
PKI
IRC
100
ISSUING APPARATUS
130
CERTIFICATE VERIFICATION PART
IRC
D B
PKI, IRC RI, RC
110
PKI
RC
IRC
KEY INFORMATION GENERATION PART
150
CERTIFICATE GENERATION PART
120
RI
300
USER APPARATUS
320
REGISTRATION INFORMATION GENERATION PART
330
CERTIFICATE VERIFICATION PART
OK
RI
RC, IRC
310
MEMORY
REGISTRATION INFORMATION RI,
REGISTRATION CERTIFICATE RC,
ISSUER REGISTRATION CERTIFICATE IRC

FIG. 13

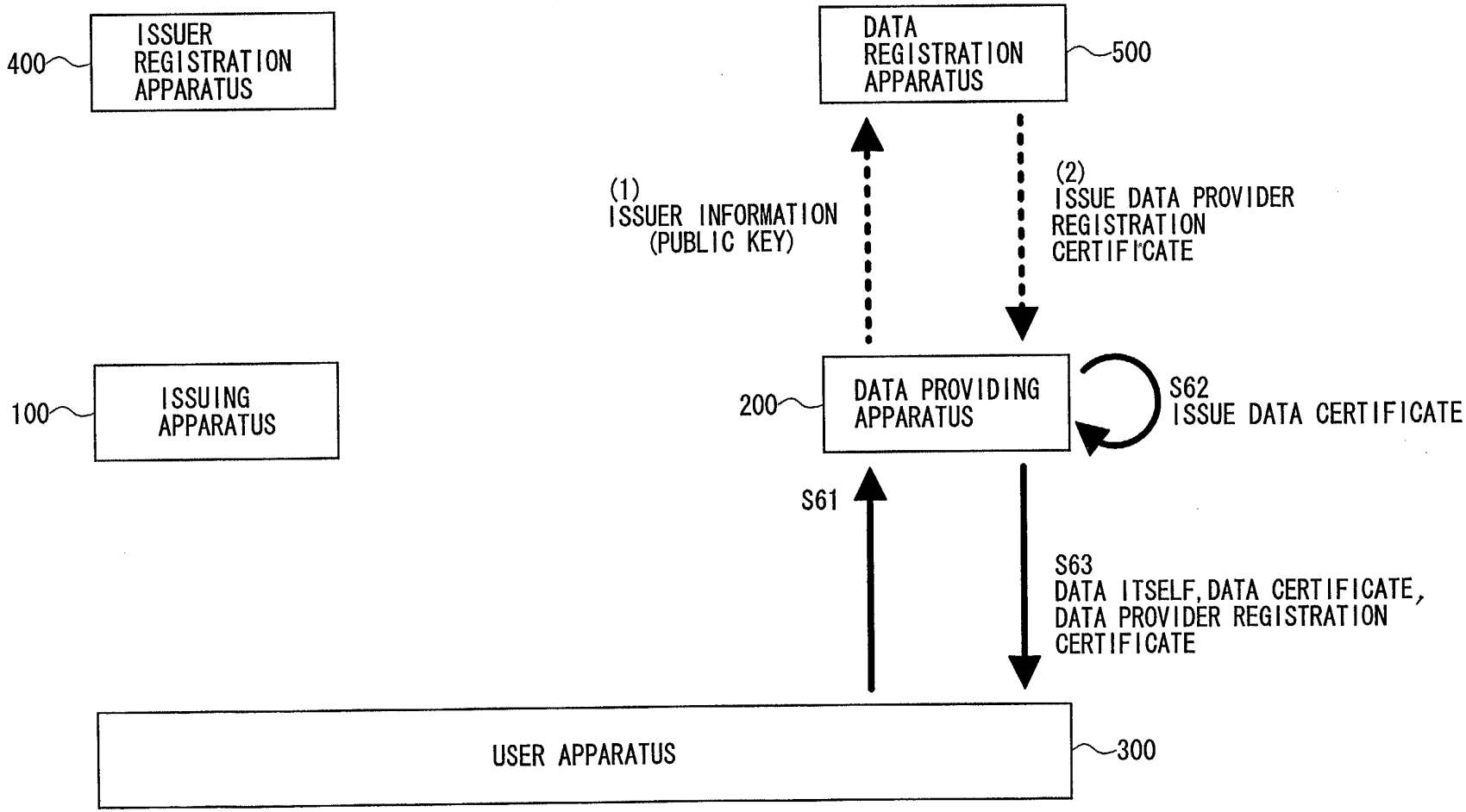

400
ISSUER REGISTRATION APPARATUS
DATA REGISTRATION APPARATUS
500
(1)
ISSUER INFORMATION (PUBLIC KEY)
(2)
ISSUE DATA PROVIDER REGISTRATION CERTIFICATE
100
ISSUING APPARATUS
200
DATA PROVIDING APPARATUS
S62
ISSUE DATA CERTIFICATE
S61
S63
DATA ITSELF, DATA CERTIFICATE, DATA PROVIDER REGISTRATION CERTIFICATE
USER APPARATUS
300

FIG. 14

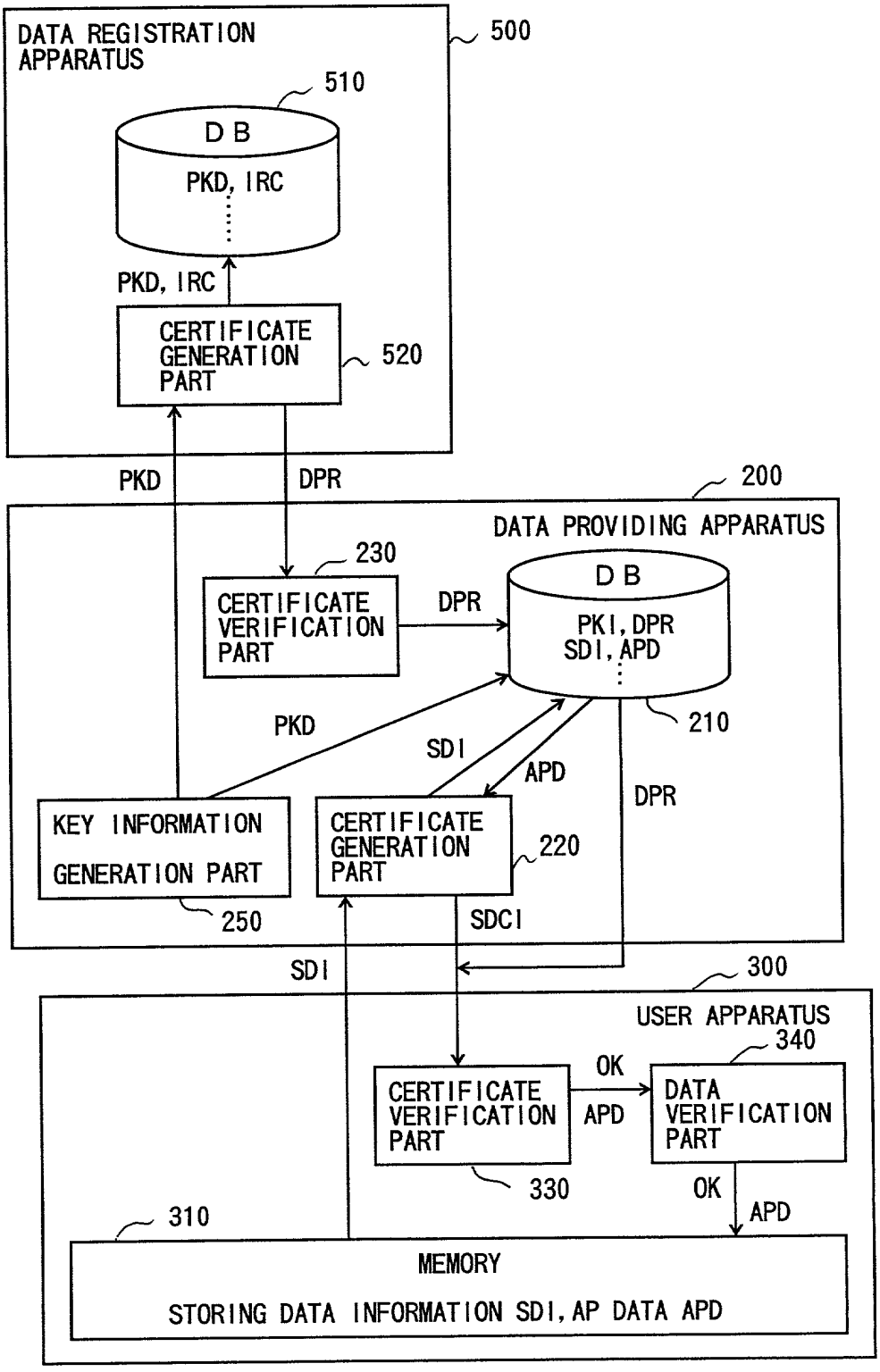

DATA REGISTRATION APPARATUS
500
510
D B
PKD, IRC
PKD, IRC
CERTIFICATE GENERATION PART
520
PKD
DPR
200
DATA PROVIDING APPARATUS
230
CERTIFICATE VERIFICATION PART
DPR
D B
PKI, DPR SDI, APD
210
PKD
SDI
APD
DPR
KEY INFORMATION GENERATION PART
250
CERTIFICATE GENERATION PART
220
SDCI
SDI
300
USER APPARATUS
340
CERTIFICATE VERIFICATION PART
330
OK
APD
DATA VERIFICATION PART
OK
APD
310
MEMORY
STORING DATA INFORMATION SDI, AP DATA APD

FIG. 15

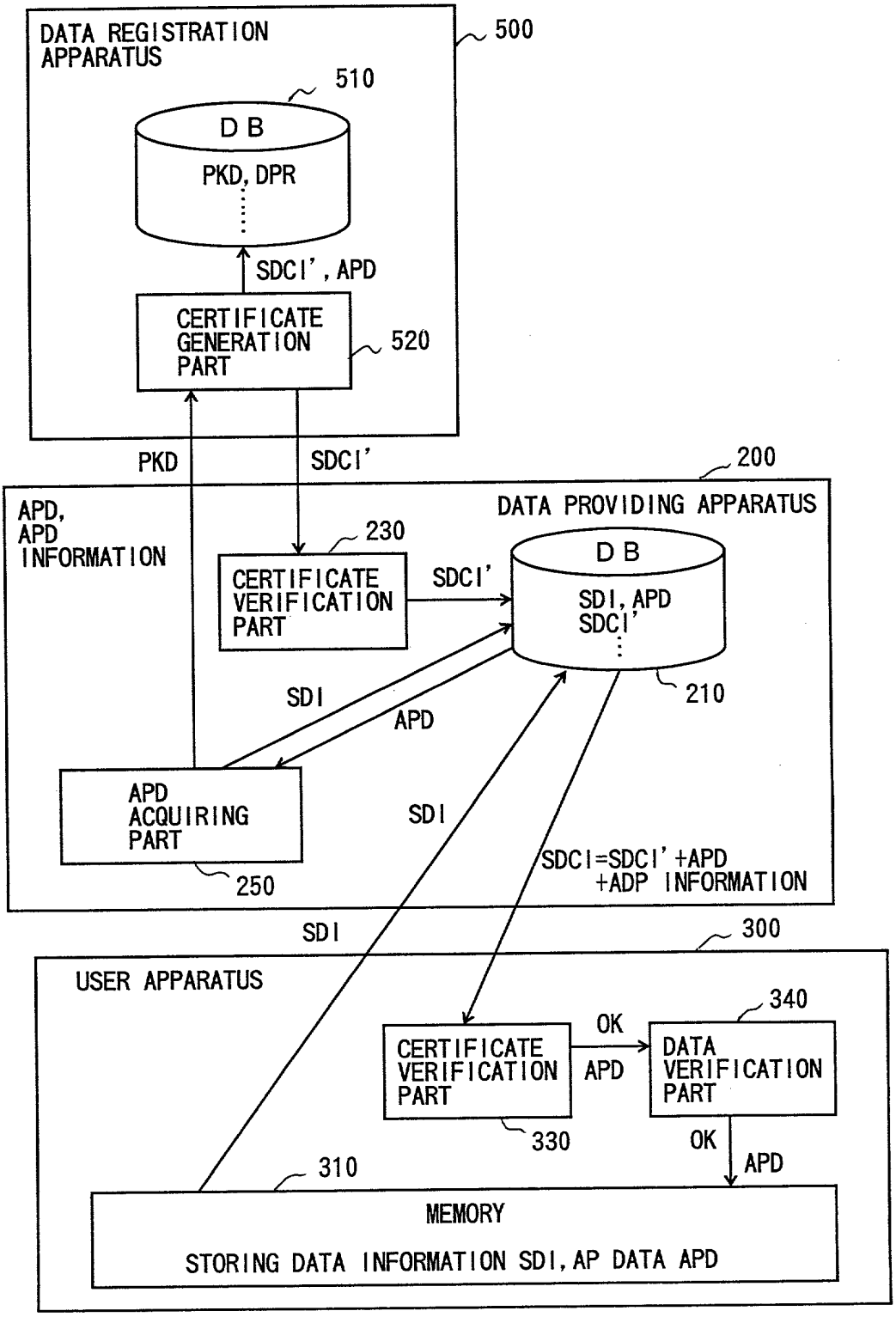
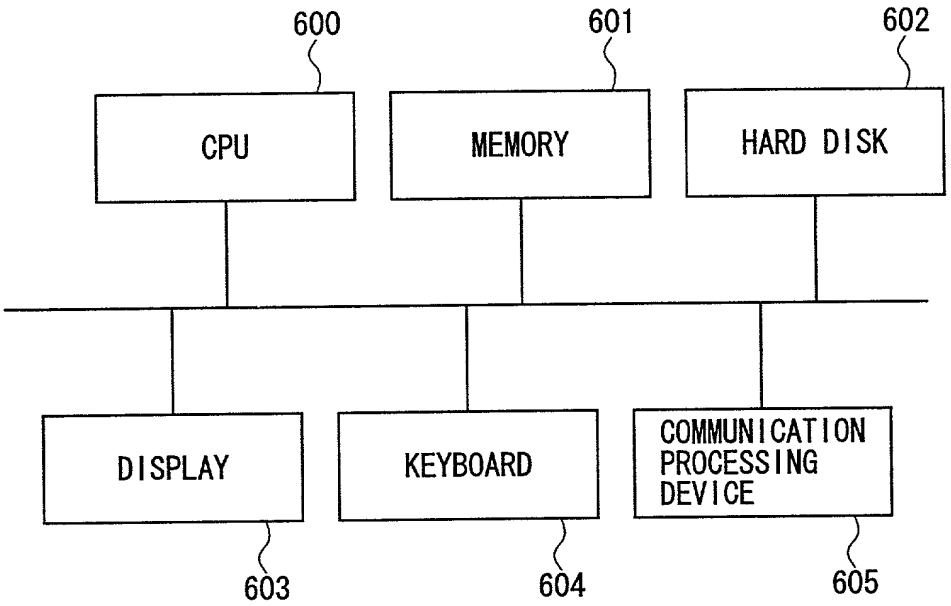

DATA REGISTRATION APPARATUS
500
510
D B
PKD, DPR
SDCI', APD
CERTIFICATE GENERATION PART
520
PKD
SDCI'
200
APD, APD INFORMATION
DATA PROVIDING APPARATUS
230
CERTIFICATE VERIFICATION PART
SDCI'
D B
SDI, APD SDCI'
210
SDI
APD
APD ACQUIRING PART
250
SDI
SDCI=SDCI'+APD +ADP INFORMATION
SDI
300
USER APPARATUS
340
CERTIFICATE VERIFICATION PART
OK
APD
DATA VERIFICATION PART
330
OK
APD
310
MEMORY
STORING DATA INFORMATION SDI, AP DATA APD

FIG. 16


600
601
602
CPU
MEMORY
HARD DISK
DISPLAY
KEYBOARD
COMMUNICATION PROCESSING DEVICE
603
604
605

DECLARATION AND POWER OF ATTORNEY – ORIGINAL APPLICATION	ATTORNEY'S DOCKET NO.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM

the specification of which

(check one)

X is attached hereto.

___ was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119
Japan	Pat. Appln. No.11-243564	30/Aug./1999		☒ YES ☐ NO
				☐ YES ☐ NO

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NO.	FILING DATE (day, month, year)	STATUS (i.e. Patented, Pending, Abandoned)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Edward W. Greason, Esq.
Reg. No. 18,918

SEND CORRESPONDENCE TO:	DIRECT TELEPHONE CALLS TO: *(name and telephone number)*
KENYON & KENYON One Broadway New York, New York 10004	Edward W. Greason (212) 425-7200 X108

(continued)

EL594605483US

201	FULL NAME OF INVENTOR	FAMILY NAME Akashika	FIRST GIVEN NAME Hideki	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY Koutou-ku	STATE OR FOREIGN COUNTRY Japan	COUNTRY OF CITIZENSHIP Japan
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY Japan
202	FULL NAME OF INVENTOR	FAMILY NAME Hirata	FIRST GIVEN NAME Shinichi	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY Zushi-shi	STATE OR FOREIGN COUNTRY Japan	COUNTRY OF CITIZENSHIP Japan
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY Japan
203	FULL NAME OF INVENTOR	FAMILY NAME Ohyama	FIRST GIVEN NAME Nagaaki	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY Kawasaki-shi	STATE OR FOREIGN COUNTRY Japan	COUNTRY OF CITIZENSHIP Japan
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY Japan
204	FULL NAME OF INVENTOR	FAMILY NAME Kokubu	FIRST GIVEN NAME Akio	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY Minato-ku	STATE OR FOREIGN COUNTRY Japan	COUNTRY OF CITIZENSHIP Japan
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY Japan
205	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
206	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Hideki Akashika	Shinichi Hirata	Nagaaki Ohyama
DATE August 22, 2000	DATE August 22, 2000	DATE August 22, 2000
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
Akio Kokubu		
DATE August 22, 2000	DATE	DATE

ATTACHMENT TO DECLARATION AND POWER OF ATTORNEY

POST OFFICE ADDRESS OF INVENTOR 201 - 204:

c/o NTT Intellectual Property Center
9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 180-8585, Japan